كيف تحمي نفسك من التتبع؟



إعداد

د. احمد عبدالله المغربي

محامي ومســـتشار قانوني

سلسلة الامتثال في إدارة القضايا المصيرية المعاصرة
سلسلة فكرية – تحليلية تُعالج الامتثال والحوكمة في:
الحركات، المؤسسات، القرار العام، والصراع السياسي.

كيف تحمي نفسك من التتبـع؟

نسخة معدلة

إعداد

د. أحمد عبد الله المغربي

دكتوراه قانون – مستشار قانوني – محامي

دورة (CAMS) مكافحة جرائم غسيل الأموال وتمويل الإرهاب

إسطنبول، الأربعاء 2026/06/17م

المحتويات

كيف تحمي نفسك من التتبع

التمهيد:

أولا/ الهاتف (الموبايل) مصدر رئيس لخطورة التتبع:

...... أما المستخدم فعليه أن يدرك أن هاتفه الذي يحمله في جيبه هو أقوى أداة تواصل في التاريخ، لكنه قد يكون أيضا أداة المراقبة الأكثر دقة. و"إيقافها عند حدها" لا يعني العزلة التقنية، بل يعني الاستخدام الواعي، فالبيانات التي يمنحها "مجانا" اليوم، هي التي ستحدد شكل مستقبله وقراراته غدا.

كن على يقين أنك مستهدف، وأنك موضع تتبع، مهما تكن مهنتك أو وظيفتك، وأينما تعيش أو تعمل، إذ الاستهداف والتتبع يقوم أولا على التسويق التجاري والاقتصادي، سواء ترويجا للسلعة، أو خلق سلعة وخلق منتجا لإشباعها.

أما إذا كنت ممكن يتخذ لنفسه هدفا ساميا في هذه الحياة، وفي هذا العالم، فأنت مخالف لما يتم التخطيط له من مراكز العالم الذي خططت للبشرية مستقبلها المظلم، وتريدها أن تبقى فيها، فإذا كنت من الفئة القليلة التي تسير عكس هذا التيار، فاعلم أن القصد الأول والمهم للتبع بقصد الاستهداف، ومنتهى التتبع حال عدم العودة الى منطقة الظلام والحياة مع القطيع، فإن حياتك هي الهدف.

وهذا لا يعني الاستسلام، بل يعني البحث عن البقاء، فأنت في صراع، ويجب أن تعرف أدوات البقاء، وهي بين يديك، وعليك فقط الاهتمام الكامل بمعرفتها وتطبيقها.

ثانيا/ الكواليس الالكترونية لزيارة الرئيس الأمريكي دونالد ترامب إلى الصين (13-15/ مايو 2026م):

ما شاهده العالم هو "معركة كسر عظم رقمية/ الكترونية"؛ الابتسامات كانت متبادلة أمام الكاميرات بين الزعيمين، لكن خلف الستار، كان الأمن الأمريكي يتعامل مع كل ما هو "صيني الصنع" على أنه قنبلة تجسس موقوتة يجب التخلص منها في القمامة قبل الإقلاع.

تفاصيل ما جرى في تلك الواقعة الحالية المثيرة للجدل، والتي تعكس ذروة "الحرب الباردة الرقمية" بين واشنطن وبكين:

ما حدث باختصار هو تطبيق بروتوكول أمني استخباراتي صارم يُعرف باسم "العزل الرقمي" (Digital Lockdown) لحماية الأمن القومي الأمريكي. واشنطن تتعامل مع الصين على أنها البيئة السيبرانية الأكثر خطورة وعدوانية في العالم، وتفترض تلقائياً أن أي جهاز يتصل بشبكة صينية أو أي مقتنى يتم استلامه هناك هو "جهاز مخترق أو ملغوم برمجياً" بشكل فوري.

تاليا تفاصيل الإجراءات الأمنية الاستثنائية التي طُبقت خلف الكواليس:

1. لِمَ لمْ يحمل ترامب وفريقه أجهزتهم المعتادة؟

- **الهواتف الشخصية بقيت في أمريكا:** تلقى الرئيس دونالد ترامب وكبار مساعديه، وحتى رؤساء الشركات الكبرى المرافقين له (مثل إيلون ماسك وتيم كوك)، تعليمات صارمة بترك هواتفهم وحواسيبهم الشخصية في الولايات المتحدة، أو إبقائها مغلقة تماماً داخل الطائرة الرئاسية (Air Force One).
- **أجهزة "نظيفة" ومؤقتة:** تم تزويد الوفد بما يُسمى "الهواتف النظيفة" أو "الهواتف الحارقة" (Burner Phones)، وهي أجهزة فارغة تماماً ومبرمجة لغرض الزيارة فقط، ولا تحتوي على أي بيانات حكومية أو حسابات بريد إلكتروني شخصية أو تطبيقات سحابية متزامنة.

- **حظر تام للشبكات المحلية:** مُع الوفد كلياً من الاتصال بشبكات "الواي فاي" في الفنادق الصينية، بل ومُنعوا حتى من استخدام منافذ الشحن (USB) العامة أو المحلية في الصين خوفاً من تقنية تُعرف باسم "Juice Jacking" (سرقة البيانات أو زرع برمجيات خبيثة عبر سلك الشحن)، واعتمدوا فقط على شواحن وبنوك طاقة أمريكية موثوقة ومفحوصة مسبقاً.
- **تغريدات ترامب:** حتى المنشورات التي ظهرت على حسابات ترامب خلال الزيارة، كانت تُدار لوجستياً من قِبل موظفين داخل واشنطن يعملون بتوقيت بكين، لحمايته من اختراق حساباته الشخصية.

2. قصة التخلص من الهدايا والشارات أسفل سلم الطائرة:

عند انتهاء الزيارة وقبل الصعود إلى الطائرة الرئاسية مغادرين بكين، رصدت التقارير الإعلامية (ومنها مراسلو البيت الأبيض ووكالة AFP) مشهداً غير مألوف:

- **شعار "ممنوع دخول أي شيء صيني للطائرة":** أُجبر أعضاء الوفد الأمريكي وحتى الصحفيين المرافقين على خلع بطاقات الاعتماد الرسمية، الشارات، الدبابيس التذكارية، ورمي الهواتف المؤقتة (Burner Phones) في سلال مهملات وُضعت خصيصاً أسفل سلم طائرة (Air Force One).
- **السبب الأمني:** هناك هاجس أمني تاريخي وقائم بأن الهدايا التذكارية، الشارات، أو الدبابيس المعدنية يمكن أن تُزرع داخلها شرائح تجسس دقيقة جداً أو ميكروفونات تنصت خفية. بما أن الطائرة الرئاسية تعتبر "منطقة عسكرية أمنية مغلقة وحساسة جداً" (SCIF)، فإن دخول أي مادة مشبوهة إليها قد يهدد أمن الاتصالات الرئاسية بالكامل.

3. الأبعاد السياسية والخلفية:

الخبراء والمحللون أشاروا إلى أن هذه الإجراءات الصارمة، وإن كانت بروتوكولاً أمنياً معتاداً في الدول ذات المخاطر الاستخباراتية العالية، إلا أنها طُبقت هذه المرة بشكل علني وحاد. ويعود ذلك إلى:

1. **انعدام الثقة المطلق:** الزيارة لم تسفر عن نتائج سياسية أو اقتصادية كبرى أو بيان مشترك ملموس، فجاء هذا التصرف الأمني ليعكس بوضوح عمق فجوة التشكيك والعداء التكنولوجي بين القوتين.
2. **الحرب السيبرانية الحالية:** تأتي الزيارة بعد تحذيرات استخباراتية أمريكية متكررة من مجموعات قراصنة صينيين (مثل Volt Typhoon و Salt Typhoon) المتهمة باختراق البنية التحتية للاتصالات الأمريكية.

4. الغرفة الامنة المحمولة:

- الغرفة الآمنة المحمولة تُعرف رسمياً في الأوساط الاستخباراتية الأمريكية باسم SCIF اختصاراً لـ (Sensitive Compartmented Information Facility). هي عبارة عن منشأة مؤقتة مضادة للتجسس الإلكتروني والصوتي، يتم شحنها وتركيبها فوراً في أي جناح فندقي أو موقع ينزل فيه الرئيس الأمريكي أو كبار قادته أثناء سفرهم خارج الولايات المتحدة. تهدف هذه الغرفة لعزل المسؤول تماماً عن البيئة المحيطة، وتمكينه من قراءة التقارير شديدة السرية أو إدارة العمليات العسكرية الحساسة دون أي خطر للاختراق.
- من أشهر الأمثلة التاريخية عليها، الصورة التي نشرها البيت الأبيض للرئيس الأسبق باراك أوباما عام 2011 وهو يدير ضربات عسكرية في ليبيا من داخل خيمة أمنية نُصبت له خصيصاً داخل غرفته بفندق في البرازيل، وكذلك استخدامها المتكرر من قِبل دونالد ترامب في منتجعاته.

- تعتمد هذه الغرف التكنولوجية على بروتوكولات ومواصفات صارمة تشمل:

أ. **العزل الفيزيائي والإلكتروني (قفص فاراداي):**

❖ درع خارجي: تُبنى الغرفة أو الخيمة المحمولة من ألياف ومواد معدنية مرنة متطورة تعمل كـ "قفص فاراداي" (Faraday Cage).

❖ حجب الإشارات: يقوم هذا الدرع بمنع دخول أو خروج أي موجات كهرومغناطيسية؛ مما يعني شلل تام لشبكات الخلوي (G/5G4)، الواي فاي، البلوتوث، وإشارات الأقمار الصناعية داخل الغرفة.

ب. **الحماية من التنصت الصوتي والليزري:**

❖ جدران عازلة للصوت: يتم تدعيمها بمواد تمنع تسرب الأصوات إلى الخارج.

❖ أجهزة التشويش الصوتي: تُثبت على جدرانها الخارجية أجهزة تُصدر اهتزازات وترددات صوتية بيضاء (White Noise). هذا الإجراء يُفشل أي محاولة للتنصت من خلال توجيه أشعة الليزر نحو نوافذ الفندق الخارجية لالتقاط ذبذبات الصوت من زجاج الغرفة.

ت. **الفحص والتعقيم الهيكلي (TCSM):**

❖ بيئة خالية من النوافذ: يفضل الخبراء دائماً نصب هذه الخيام الأمنية في غرف داخلية عميقة أو قاعات مؤتمرات بالفنادق لا تحتوي على نوافذ تطل على الشارع.

❖ التفتيش الإلكتروني: قبل تركيب الغرفة، يمسح عملاء الخدمة السرية الجناح الفندقي كاملاً بأجهزة كشف متطورة للتأكد من عدم وجود ميكروفونات أو كاميرات تجسس مخفية في الجدران أو التوصيلات الكهربائية التابعة للفندق.

ث. **قنوات اتصال مشفرة ومستقلة:**

❖ خطوط عسكرية: لا تعتمد الغرفة على أي بنية تحتية للبلد المضيف؛ بل ترتبط مباشرة بالطائرة الرئاسية (Air Force One) أو بسيارات الاتصال المرافقة للوفد عبر كابلات ألياف ضوئية مؤمنة ومضادة للقطع والتنصت.

❖ أجهزة اتصال خاصة: تحتوي الغرفة على شاشات وهواتف حمراء مشفرة تتصل بالبيت الأبيض والبنتاغون عبر أقمار صناعية عسكرية أمريكية حصراً.

ج. **حظر مطلق للأجهزة الشخصية:**

❖ خزائن عند الباب: يمنع منعاً باتاً دخول أي شخص –حتى الرئيس نفسه– وهو يحمل هاتفاً ذكياً، أو ساعة ذكية، أو سماعات لاسلكية، أو أي جهاز إلكتروني شخصي. تُترك هذه الأجهزة في صناديق مغلقة خارج الخيمة لحماية الغرفة من أي برمجيات خبيثة قد تكون كامنة في تلك الأجهزة الشخصية.

هذه محاولة ارشادية تقدم لك الأدوات اللازمة لتكسب معركتك مع المتربصين المتصيدين، فادخل في هذا الجو بإرادة البقاء والاستمرار والنضال والانتصار.

المحور الأول: في التتبع وأحواله وادواته ومخاطره

تعريفات:

1-التتبع الالكتروني الأمني:

التتبع الإلكتروني الأمني: استخدام تقنيات وأدوات رقمية لمراقبة وإدارة المواقع أو الأنشطة أو البيانات بهدف تحقيق الحماية وضمان الامتثال للأنظمة. يتخذ هذا التتبع عدة أشكال تختلف باختلاف الغرض منه، سواء أكان لأغراض أمنية عامة، رقابية، أم حتى كتهديد للأمن السيبراني.

التتبع الإلكتروني الأمني للأفراد: استخدام تقنيات حديثة (مثلGPS) ، بيانات الهواتف، وشرائح التعريف (لرصد تحركات الأفراد ومواقعهم لحظياً. يهدف هذا الإجراء، الذي يتم غالباً بناءً على إذن قانوني، إلى تعزيز الأمن، ومراقبة الأشخاص الخاضعين لإجراءات قضائية، أو ضمان سلامة أفراد محددين، مما يوفر بيانات دقيقة للأجهزة الأمنية .

أبرز أنواع التتبع الإلكتروني الأمني:

- **تتبع الموقع الجغرافي (GPS Tracking):** استخدام الأقمار الصناعية أو شبكات الاتصالات لتحديد المواقع الدقيقة للمركبات، البضائع، أو الأفراد.
- **المراقبة الإلكترونية للأشخاص:** استخدام تطبيقات الهواتف، كاميرات التعرف على الوجه، أو "الأساور الإلكترونية" لمتابعة الأشخاص الخاضعين للمراقبة الأمنية أو السلطات.
- **تتبع البيانات والمنتجات (الرقابة اللوجستية):** أنظمة تتبع تضمن سلامة ومصدر المنتجات (مثل الأدوية) من التصنيع حتى المستهلك لمنع التلاعب.
- **التتبع في الأمن السيبراني:** مراقبة الأنشطة على الشبكات والأنظمة لاكتشاف الاختراقات والتهديدات الأمنية ومنع الوصول غير المصرح به للمعلومات الحساسة .

الأهداف الأساسية:

1. **حماية المجتمع:** من خلال تعزيز الرقابة والتأكد من سلامة المواد الحساسة.
2. **الأمن الجنائي:** متابعة الأفراد والكيانات لضمان عدم خرق القوانين أو الهرب من العدالة.
3. **حماية الخصوصية الرقمية:** الكشف عن محاولات التتبع المجهولة أو غير المصرح بها للأجهزة الشخصية.
4. **إدارة الأصول:** متابعة أداء ومواقع الفرق الأمنية أو أساطيل المركبات لضمان كفاءة العمل.

الأدوات والتقنيات المستخدمة

- **الأقمار الصناعية وشبكات المحمول:** لتحديد الإحداثيات الجغرافية بدقة.
- **ملفات تعريف الارتباط (Trackers):** لجمع بيانات السلوك الرقمي عبر الإنترنت.
- **تطبيقات الهواتف الذكية:** التي ترسل تحديثات لحظية للموقع والسرعة .

جوانب ومكونات التتبع الإلكتروني الأمني:

- **الأدوات والتقنيات:** تعتمد على نظام تحديد المواقع العالمي(GPS) ، التقاط إشارات الهواتف الذكية، واستخدام شرائح الهاتف النقال (SIM cards) لتحديد موقع المتهم أو الضحية بدقة.
- **المراقبة القضائية:** يُستخدم كبديل للتوقيف القضائي، حيث يُفرض على المحكوم عليهم ارتداء أجهزة تتبع لتحديد نطاقهم الجغرافي وحركتهم.

- **استخدامات أمنية وجنائية:** يستخدم في التحقيقات الجنائية، تحديد مواقع الخلايا الإرهابية، وتعقب الأفراد في قضايا الاختطاف.
- **الأمن الشخصي والأسري:** توفر تقنيات الـ GPS حلولاً للأفراد لتتبع ومراقبة أطفالهم أو أقاربهم المسنين لضمان سلامتهم.
- **مشروعية الإجراءات:** يجب أن يتم التتبع وفقاً لإذن قانوني من جهات مختصة، حيث تُعتبر البيانات دليلاً قوياً أمام القضاء إذا تم جمعها قانونياً.

الهدف من التتبع الإلكتروني:

أ. **تعزيز السلامة:** الحد من الجرائم وتحديد مواقع الأفراد في حالات الطوارئ.

ب. **الرقابة:** متابعة تحركات الأفراد المشبوهين أو الخاضعين للإقامة الجبرية.

2- التتبع الالكتروني الاستخباراتي:

التتبع الإلكتروني الاستخباراتي: عملية جمع، تحليل، ورصد المعلومات باستخدام وسائل تقنية متطورة لتحديد مواقع، تحركات، ونشاطات أشخاص أو كيانات مستهدفة.

تُستخدم هذه الأساليب من قبل أجهزة الاستخبارات، وقوات إنفاذ القانون، وحتى المهاجمين الإلكترونيين لتعقب الأهداف بدقة عالية، وتشمل مراقبة الهواتف، الإنترنت، والبنية التحتية الرقمية .

تفصيل لطرق وأدوات التتبع الاستخباراتي:

- **تتبع الهواتف الذكية (Mobile Tracking):** تلجأ أجهزة الاستخبارات إلى اختراق أبراج الاتصالات لتحديد مواقع الهواتف النقالة للمشتبه بهم بدقة، كما يتم تتبع المكالمات والرسائل النصية.
- **الاستخبارات مفتوحة المصدر(OSINT):** جمع وتحليل المعلومات المتاحة للجمهور (على الإنترنت ووسائل التواصل الاجتماعي) لاستخلاص رؤى قيمة.
- **تتبع عناوين IP:** تحديد الموقع الجغرافي للمستخدمين من خلال عنوان الاتصال بالشبكة IP) (Address الخاص بجهاز الكمبيوتر أو الهاتف.
- **التجسس عبر البرمجيات الخبيثة:** اختراق الأجهزة باستخدام برمجيات متطورة لسرقة البيانات أو تفعيل الكاميرا والميكروفون.
- **استخدام الطائرات المسيرة (Drones):** تلعب دوراً رئيسياً في مراقبة وتحليل تحركات الأهداف على الأرض.
- **تتبع عبر الألعاب الإلكترونية:** قد تُستخدم تطبيقات الألعاب كأدوات استخباراتية لجمع بيانات عن المستخدمين ومعرفة مواقعهم.

الأهداف الرئيسية للتتبع الاستخباراتي:

1. **الأمن القومي:** تحديد مواقع المتطرفين والمطلوبين.
2. **الأمن السيبراني:** تتبع مؤشرات الاختراق (IOCs) والتهديدات النشطة.
3. **الاستخبارات التشغيلية:** مراقبة الأنشطة المباشرة لاتخاذ إجراءات مضادة فورية.

تتطور هذه الأدوات باستمرار مع التطور التكنولوجي، مما يجعلها سلاحاً ذا حدين يستخدم للأمن الداخلي والخارجي، وكذلك في التجسس الإلكتروني.

ما هي أكثر الدول استخداما للتتبع الالكتروني الاستخباراتي؟؟

تتصدر الولايات المتحدة الأمريكية والصين وروسيا وإسرائيل قائمة أكثر الدول استخداماً وتطويراً لتقنيات التتبع الإلكتروني الاستخباراتي على مستوى العالم. تعتمد هذه الدول على ميزانيات ضخمة وبنى تحتية تكنولوجية متقدمة لجمع المعلومات عبر الفضاء السيبراني.

فيما يلي تفصيل لأبرز هذه الدول وقدراتها الاستخباراتية الإلكترونية:

القوى العظمى في التتبع الإلكتروني:

- **الولايات المتحدة الأمريكية:** تُعد الزعيم بلا منازع في هذا المجال؛ حيث تخصص ميزانية سنوية تزيد عن 72 مليار دولار لتطوير القدرات السيبرانية. تمتلك وكالات مثل "وكالة الأمن القومي" (NSA) و"وكالة الاستخبارات المركزية" (CIA) قدرات هائلة على جمع المعلومات الاستخباراتية وتتبع الأهداف عالمياً.
- **الصين:** تبرز كعملاق رقمي يدير أكبر نظام للمراقبة والترصد في العالم. تمتلك الصين جيشاً إلكترونياً منظماً وتدير ما لا يقل عن 245 قمراً اصطناعياً مخصصاً للدفاع والتجسس، منها 81 قمراً مصمماً خصيصاً للاستخبارات الإلكترونية ورصد الإشارات.
- **روسيا:** تمتلك "جهاز الأمن الفيدرالي" (FSB) الذي يتمتع بقدرات استثنائية في تتبع المعلومات والتحقيق في الجرائم السيبرانية الخطيرة. تشتهر روسيا عالمياً بقدراتها الهجومية الضخمة في الحرب الإلكترونية.
- **إسرائيل:** تُعرف بكونها رائدة في تصدير تقنيات التجسس المتطورة. يتخصص جهاز "الموساد" ووحدات الاستخبارات التقنية (مثل الوحدة 8200) في جمع المعلومات الخارجية وتنفيذ عمليات سيبرانية معقدة.
- **المملكة المتحدة:** شريك أساسي في شبكة "العيون الخمس" الاستخباراتية، وتمتلك مركز (GCHQ) الذي يعد من أقوى مراكز الحماية والمراقبة في أوروبا.
- **فرنسا وألمانيا:** تمتلكان بنى تحتية استخباراتية متطورة تخدم الأمن القومي ومكافحة التهديدات الرقمية في الاتحاد الأوروبي.
- **الهند وكوريا الجنوبية:** تشهد الهند توسعاً سريعاً في نشاطها السيبراني، بينما تركز كوريا الجنوبية على مواجهة التهديدات السيبرانية المستمرة بقدرات دفاعية وتتبعية عالية.

القوى الصاعدة عربياً (في الأمن السيبراني والجاهزية):

وفقاً لمؤشر الأمن السيبراني العالمي لعام 2024، حققت عدة دول عربية مراتب متقدمة في الجاهزية الرقمية والأطر التقنية، مما يعكس تطوراً في قدراتها الاستخباراتية الدفاعية:

- **المملكة العربية السعودية:** حققت المرتبة الأولى عالمياً في مؤشر الأمن السيبراني ضمن تقرير التنافسية العالمية لعام 2024.
- **الإمارات العربية المتحدة:** تُعد من الدول المرجعية في الأمن السيبراني وتمتلك أطراً تقنية وتنظيمية متكاملة.
- **مصر والأردن وقطر وسلطنة عمان:** صُنفت ضمن المستوى الأعلى في الجاهزية السيبرانية، مما يعزز قدرتها على المراقبة وحماية فضائها الرقمي.

برامج التجسس المحددة التي تستخدمها الوكالات الاستخباراتية وطرق الحماية منها:

تستخدم وكالات الاستخبارات برمجيات تجسس متطورة للغاية تعتمد على ثغرات "يوم الصفر" (Zero–day) لاختراق الأجهزة دون أي تفاعل من المستخدم. وتعد شركات التقنيات الهجومية، خاصة الإسرائيلية والأمريكية، المورد الرئيسي لهذه الأدوات للحكومات عالمياً.

أبرز برامج التجسس الاستخباراتية النشطة (2024–2026)

- **Pegasus (بيغاسوس):** من تطوير شركة NSO Group، وهو الأكثر شهرة وقدرة على اختراق هواتف Android وiOS عبر هجمات "النقر الصفري" (Zero–click). يسمح للمشغلين بالتنصت على المكالمات، ونسخ الرسائل المشفرة، وحتى إرسال رسائل مزيفة من جهاز الضحية.
- **Graphite (غرافايت):** برنامج "شبح" من تطوير شركة Paragon Solutions. يتميز باستراتيجية العمل تحت الرادار، ويستهدف الهواتف المشفرة وسحب البيانات من الخدمات السحابية (Cloud).
- **Landfall (لاندفول):** برمجية تجسس حديثة تم اكتشافها في 2024–2025 تستهدف هواتف Samsung Galaxy تحديداً عبر ثغرات معقدة في معالجة الصور، مما يسمح بالاختراق الصامت بمجرد استلام صورة مفخخة.
- **StealerBot (ستيلر بوت):** أداة تجسس متقدمة تستخدمها مجموعات التهديد (مثل SideWinder) لاستهداف الكيانات الحكومية في الشرق الأوسط وأفريقيا، وتتميز بقدرة فائقة على الاختباء داخل النظام.
- **Predator (بريداتور):** تطوره شركة Cytrox/Intellexa، ويستخدم لجمع البيانات الجغرافية والصوتية من الأجهزة المستهدفة.

كيفية الحماية من التجسس الاستخباراتي

نظراً لتعقيد هذه البرامج، تتطلب الحماية اتباع استراتيجية دفاعية متعددة الطبقات:

- **تفعيل وضع الأمان المشدد (Lockdown Mode):** في هواتف iPhone، يقلل هذا الوضع بشكل كبير من "سطح الهجوم" عبر تقييد ميزات مثل معاينة الرسائل وتشغيل الأكواد البرمجية المريبة.
- **تحديث النظام الفوري:** سد الثغرات الأمنية (مثل CVE–2025–21042) هو الخط الدفاعي الأول؛ حيث تُعالج التحديثات نقاط الضعف التي تستغلها هذه البرمجيات.
- **استخدام تطبيقات الحماية المتخصصة:**
    - ❖ Antivirus AI & Anti Spy: برامج تعتمد على الذكاء الاصطناعي لرصد السلوكيات الشاذة ومؤشرات الاختراق (IoC) بدقة تصل إلى 99.8%.
    - ❖ TotalAV & Bitdefender: توفر طبقات حماية متقدمة ضد الروتكيت (Rootkit) والبرمجيات الهجينة.
- **تجنب "كسر الحماية" (Root/Jailbreak):** الهواتف التي تم كسر حمايتها تصبح أكثر عرضة لتطبيقات التجسس التي يمكنها حينئذٍ الوصول للميكروفون والكاميرا والرسائل المشفرة بسهولة أكبر.
- **اعتماد نموذج "الثقة الصفرية" (Zero Trust):** افتراض أن أي جهاز أو اتصال قد يكون غير موثوق، واستخدام تقنيات التشفير القوي وإدارة الهوية الموحدة.

مؤشرات الاختراق وكيفية الفحص الشامل له وكيفية عزله:

أولاً: العلامات التحذيرية لاختراق الجهاز (مؤشرات الاختراق):

إذا لاحظت اجتماع أكثر من علامة من هذه العلامات، فقد يكون جهازك مستهدفاً:

1. **استنزاف البطارية المفاجئ:** برامج التجسس تعمل في الخلفية باستمرار لإرسال البيانات، مما يؤدي لهبوط مستوى البطارية بشكل أسرع من المعتاد دون استخدام مكثف.
2. **ارتفاع حرارة الجهاز:** سخونة الهاتف وهو في وضع الخمول أو في جيبك تشير إلى وجود عمليات معالجة قوية تجري بالخلفية.
3. **زيادة استهلاك البيانات (Data):** ارتفاع مفاجئ وغير مبرر في استهلاك بيانات الإنترنت (Mobile Data)، ناتج عن رفع الملفات والصور والتسجيلات إلى سيرفرات التجسس.
4. **سلوكيات غريبة للتطبيقات:** فتح الكاميرا أو الميكروفون تلقائياً (ظهور النقطة الخضراء أو البرتقالية في أعلى الشاشة دون سبب)، أو إعادة تشغيل الجهاز بشكل مفاجئ.
5. **رسائل نصية مشبوهة:** تلقي رسائل تحتوي على روابط غريبة أو رموز غير مفهومة؛ فبرامج التجسس الحديثة تستخدم هذه الرسائل كـ "ناقل" للاختراق الصامت.

ثانياً: كيفية إجراء فحص أمني شامل (خطوات عملية):

للتأكد من نظافة جهازك، اتبع المسارات التالية من الأبسط إلى الأكثر تعقيداً:

1.الفحص عبر تطبيقات الحماية (المستوى الأول):

- ستخدم تطبيقات موثوقة مثل Malwarebytes أو Bitdefender أو Avast لإجراء فحص كامل لملفات النظام والتطبيقات المثبتة.
- بالنسبة لهواتف Android، تأكد من تفعيل خاصية Google Play Protect.

2. استخدام أداة MVT (المستوى المتقدم – للمحترفين):

- طورت منظمة العفو الدولية أداة تسمى Mobile Verification Toolkit (MVT). هي أداة تقنية متقدمة مخصصة لكشف آثار برمجيات مثل "بيغاسوس" و"بريداتور" عبر فحص سجلات الجهاز (Logs) والنسخ الاحتياطية.

3. فحص صلاحيات التطبيقات:

- ادخل إلى الإعدادات -> الخصوصية -> مدير الأذونات (Permission Manager).
- راجع التطبيقات التي تملك صلاحية الوصول إلى الميكروفون، الكاميرا، والموقع الجغرافي. أي تطبيق مجهول يمتلك هذه الصلاحيات يجب حذفه فوراً.

4. فحص استهلاك البطارية والبيانات:

- راقب قائمة التطبيقات الأكثر استهلاكاً للبطارية في الإعدادات. إذا وجدت تطبيقاً لا تستخدمه يستهلك نسبة كبيرة، فهذا مؤشر خطر.

5. فحص الروابط المشبوهة:

- إذا وصلك رابط تشك فيه، لا تفتحه. استخدم موقع VirusTotal لفحص الرابط والتأكد مما إذا كان مرتبطاً بسيرفرات خبيثة قبل النقر عليه.

نصيحة وقائية ذهبية:

الحل الأكثر فعالية ضد هجمات "النقر الصفري" الاستخباراتية هو إعادة تشغيل الجهاز يومياً.

برمجيات التجسس الحديثة غالباً ما تعيش في "الذاكرة المؤقتة"، وإعادة التشغيل تؤدي في كثير من الأحيان إلى قطع اتصالها وإجبار المهاجم على محاولة الاختراق من جديد، مما يزيد من فرص اكتشافه.

ثالثا: الخطوات الفورية التي يجب اتخاذها إذا تأكدت من وجود اختراق، مثل كيفية عزل الجهاز أو تأمين الحسابات الحساسة؟

إذا تأكدت أو شككت بقوة في وجود اختراق استخباراتي لجهازك، يجب أن تتحرك بسرعة وبشكل منهجي لمنع تسريب المزيد من البيانات. إليك الخطوات الفورية والعملية:

1. عزل الجهاز فوراً:

- **تفعيل وضع الطيران:** اقطع جميع الاتصالات (Wi-Fi، بيانات الهاتف، والبلوتوث). برامج التجسس تعتمد على الإنترنت لإرسال بياناتك للمهاجم، وبقطع الاتصال "تشل" حركة البرنامج.
- **إزالة شريحة الـ SIM:** في الحالات الحساسة، يفضل إخراج الشريحة لمنع تتبع الموقع عبر أبراج الاتصالات.

2. تأمين الحسابات (من جهاز آخر نظيف):

لا تغير كلمات مرورك من الجهاز المخترق أبداً. استخدم جهازاً موثوقاً للقيام بما يلي:

- **تسجيل الخروج من كافة الأجهزة:** ادخل إلى إعدادات الأمان في Google، iCloud، ومنصات التواصل، واختر "تسجيل الخروج من جميع الجلسات النشطة".
- **تغيير كلمات المرور: ابدأ بالحسابات الأساسية (البريد الإلكتروني، البنك) واستخدم كلمات مرور قوية** وفريدة.
- ت**فعيل المصادقة الثنائية (FA2):** استخدم تطبيقات مثل Google Authenticator بدلاً من الرسائل النصية (SMS)، لأن المخترق قد يتمكن من قراءة رسائلك.

3. التعامل مع الجهاز المخترق:

- **لا تعتمد على "إعادة ضبط المصنع" (Factory Reset) وحدها:** برمجيات التجسس الاستخباراتية المتطورة قد تختبئ في مستويات عميقة من النظام (Root) وتظل موجودة حتى بعد الفورمات.
- **تحديث النظام بالكامل:** إذا كان لا بد من استخدام الجهاز، قم بتحميل أحدث إصدار من نظام التشغيل عبر وضع الاسترداد (Recovery Mode) لضمان استبدال ملفات النظام المصابة.
- **في الحالات القصوى:** إذا كنت مستهدفاً بشكل شخصي من جهة استخباراتية، فإن النصيحة الأمنية هي التخلص من الجهاز تماماً وشراء جهاز جديد، لأن بعض الثغرات تكون على مستوى العتاد (Hardware).

4. حماية البيانات الحساسة:

- **التشفير:** تأكد من أن جميع ملفاتك المهمة مشفرة.
- **مراقبة النشاط المالي:** راقب كشوف حساباتك البنكية لأي عمليات غير مصرح بها.

5. إجراء فحص جنائي (اختياري):

إذا كنت تحتاج لإثبات الاختراق قانونياً، لا تمسح بيانات الجهاز. سلمه لجهة تقنية متخصصة لاستخراج الأدلة الرقمية باستخدام أدوات مثل MVT التي ذكرناها سابقاً.

نصيحة للمستقبل: انتقل لاستخدام تطبيقات مراسلة أكثر أماناً وتشفيراً مثل Signal، وقم بتفعيل خاصية "الرسائل المختفية" تلقائياً.

كيفية ضبط إعدادات الخصوصية القصوى في تطبيقات المراسلة مثل Signal أو WhatsApp لتقليل احتمالية تتبعك مستقبلاً:

1. تطبيق سيجنال (Signal) – الخيار الأكثر أماناً:

يُعد الأفضل عالمياً لأن بياناتك لا تُخزن على خوادمه. قم بتفعيل الآتي:

- **قفل التسجيل (Registration Lock):** يمنع أي شخص من إعادة تسجيل رقمك على جهاز آخر بدون رقم التعريف الشخصي (PIN).
- **الرسائل المختفية (Disappearing Messages):** اجعلها الخيار الافتراضي لكل المحادثات (مثلاً بعد يوم أو أسبوع). هذا يضمن عدم وجود أرشيف رسائل يمكن استخراجه في حال فُقد الجهاز أو تم اختراقه.
- **تأمين الشاشة (Screen Security):** يمنع أخذ "لقطات شاشة" (Screenshots) للمحادثات ويحجب معاينة التطبيق في قائمة التطبيقات المفتوحة.
- **ترحيل المكالمات (Relay Calls):** (إعداد مهم جداً) يمرر مكالماتك عبر خوادم Signal لإخفاء عنوان الـ IP الخاص بك عن الطرف الآخر، مما يمنع تحديد موقعك الجغرافي أثناء المكالمة.

2. تطبيق واتساب (WhatsApp):

رغم كونه مشفراً، إلا أنه يجمع "بيانات وصفية" (Metadata). لتقليل ذلك:

- **النسخ الاحتياطي المشفر (End-to-end Encrypted Backup):** مفعل اختيارياً؛ إذا لم تفعله بكلمة مرور خاصة، يمكن لوكالات الاستخبارات الوصول لرسائلك عبر طلب النسخة الاحتياطية من Google Drive أو iCloud.
- **إسكات المتصلين المجهولين (Silence Unknown Callers):** يقلل من خطر هجمات "النقر الصفري" التي تبدأ بمكالمة من رقم غريب.
- **حماية عنوان IP في المكالمات:** تفعيل هذا الخيار (موجود في إعدادات الخصوصية -> متقدم) يجعل مكالماتك تمر عبر خوادم شركة Meta لإخفاء موقعك.
- **التحقق بخطوتين (Two-Step Verification):** لضمان عدم سحب الحساب من جهاز آخر.

3. إعدادات عامة للهاتف (Android & iOS):

- **تعطيل الوصول للموقع (GPS):** قم بإيقاف "خدمات الموقع" لجميع التطبيقات، ومنحها فقط عند الضرورة القصوى.

- **مراجعة "الوصول الخاص":** ابحث في إعدادات الهاتف عن "تطبيقات مشرف الجهاز" (Device Admin Apps) وتأكد من عدم وجود أي تطبيق مجهول يملك صلاحية التحكم في الهاتف.
- **استخدام VPN موثوق:** استخدم خدمات مثل (ProtonVPN) لتشفير حركة مرور الإنترنت بالكامل وإخفاء هويتك عن مزود خدمة الإنترنت المحلي.

تذكر دائماً: برمجيات التجسس الاستخباراتية تستهدف "الثغرات" وليس "التشفير"؛ لذا فإن تطبيقاً مؤمناً على نظام تشغيل غير مُحدث يظل عرضة للخطر.

بعض الهواتف أو أنظمة التشغيل البديلة التي يفضلها خبراء الأمن لضمان خصوصية أعلى من الهواتف التقليدية:

للباحثين عن أقصى درجات الخصوصية، يبتعد الخبراء غالباً عن الأنظمة التقليدية (أندرويد الخام وiOS) ويتجهون إلى خيارات تمنح المستخدم سيطرة كاملة على العتاد والبرمجيات:

1. أنظمة التشغيل الأكثر أماناً (لأجهزة أندرويد محددة):

هذه الأنظمة تُثبت عادةً على أجهزة Google Pixel لأنها توفر أفضل معايير أمان للعتاد (Hardware Security):

- **GrapheneOS:** يعتبر "المعيار الذهبي" حالياً. هو نظام مفتوح المصدر يركز على الخصوصية، ويقوم بعزل التطبيقات بشكل صارم جداً، ولا يحتوي على خدمات جوجل بشكل افتراضي (مما يمنع تتبع الشركة لك). يتميز بخاصية "Network Sandboxing" التي تمنع التطبيقات من الوصول للإنترنت دون إذن صريح.
- **CalyxOS:** خيار ممتاز يركز على سهولة الاستخدام مع الحفاظ على الخصوصية، ويأتي مدمجاً مع أدوات مثل Signal وTor وDuckDuckGo بشكل افتراضي.

2. الهواتف ذات "المفاتيح الفيزيائية" (Hardware Kill Switches):

هذه الهواتف مصممة لمنع التجسس الاستخباراتي "مادياً" عبر مفاتيح حقيقية على جسم الهاتف:

- **Purism Librem 5:** هاتف يعمل بنظام PureOS (لينكس). يحتوي على مفاتيح فيزيائية تتيح لك قطع الكهرباء تماماً عن الكاميرا، الميكروفون، والواي فاي/ البلوتوث. حتى لو تم اختراق النظام برمجياً، لن يتمكن المخترق من تشغيل الميكروفون لأن الدائرة الكهربائية مقطوعة يدوياً.
- **PinePhone / PinePhone Pro:** هاتف مشابه موجه للمطورين والمتحمسين للأمن، يسمح بتبديل أنظمة تشغيل متعددة ويوفر مفاتيح قطع للعتاد تحت الغطاء الخلفي.

3. **هواتف "الأمان المطلق" (للمؤسسات والمسؤولين):**

- **Sirin Labs Finney:** هاتف يوفر طبقات حماية إضافية ونظام تشغيل مؤمن بشكل خاص ضد الهجمات السيبرانية.
- **Bittium Tough Mobile 2:** هاتف فنلندي مصمم للاستخدام العسكري والحكومي، يحتوي على وضع "السرية التامة" الذي يعطل جميع أجهزة الاستشعار والميكروفونات بلمسة واحدة.

4. وضع "الإغلاق" في آيفون (Lockdown Mode): إذا كنت تفضل البقاء مع شركة Apple، فإن Lockdown Mode هو أقوى خط دفاعي رسمي:

- هذا الوضع يعطل معظم ميزات الرسائل المعقدة، ويمنع معاينة الروابط، ويغلق ثغرات "النقر الصفري" المعروفة. هو مصمم خصيصاً لمواجهة برمجيات مثل "بيغاسوس".

5. نصيحة "الهاتف المحروق" (Burner Phone): في المهام أو المناطق عالية الخطورة، يستخدم الخبراء هواتف رخيصة جداً (غير ذكية) تُستخدم لمرة واحدة ثم يتم إتلافها، وذلك لتجنب ترك أي أثر رقمي دائم أو حسابات مرتبطة بالهوية الشخصية.

> **باختصار:** إذا كنت تريد أعلى حماية ممكنة دون التضحية بالاستخدام اليومي، فإن هاتف Google Pixel محمل عليه نظام GrapheneOS هو التوصية الأولى لخبراء الأمن السيبراني اليوم.

كيفية التثبيت واماكن الحصول على الهواتف المتخصصة؟

تثبيت أنظمة تشغيل أمنية يتطلب بعض المعرفة التقنية البسيطة، بينما الحصول على الهواتف المتخصصة يعتمد على ميزانيتك ومكان إقامتك. إليك الدليل العملي لذلك:

أولاً: كيفية تثبيت نظام GrapheneOS (الأكثر ترشيحاً):

لتثبيت هذا النظام، ستحتاج إلى جهاز Google Pixel (من إصدار 6 إلى 9) وجهاز كمبيوتر.

1. **المتطلبات:** كابل USB-C عالي الجودة، ومتصفح يدعم تقنية WebUSB (مثل Google Chrome أو Microsoft Edge).
2. **تفعيل إعدادات المطور:** اذهب إلى إعدادات الهاتف > حول الهاتف > اضغط على "رقم الإصدار" (Build Number) 7 مرات حتى يتم تفعيل خيارات المطور.
3. **فتح قفل OEM:** من خيارات المطور، قم بتفعيل "OEM Unlocking" و"USB Debugging".
4. **التثبيت عبر المتصفح:** توجه إلى الموقع الرسمي (grapheneos.org) واستخدم Web Installer. الخطوات مؤتمتة وسهلة:

- قم بتوصيل الهاتف بالكمبيوتر.
- اضغط على "Unlock Bootloader" من الموقع واتبع التعليمات على شاشة الهاتف.
- اضغط على "Install & Download" ليقوم الموقع بتحميل النظام وتثبيته تلقائياً.
- أخيراً، اضغط على "Lock Bootloader" لإعادة قفل الأمان (خطوة ضرورية جداً للأمن).

ثانياً: أماكن الحصول على الهواتف المتخصصة:

1. أجهزة Google Pixel (لتركيب GrapheneOS أو CalyxOS):

- **المصدر:** يمكنك شراؤها من متاجر Google الرسمية، أو أماكن مثل Amazon و eBay.
- **ملاحظة هامة:** تأكد من شراء النسخة "Unlocked" (غير المقفلة لشركة اتصالات معينة)؛ لأن هواتف شركات الاتصالات (مثل Verizon) غالباً ما تمنع فتح قفل الـ Bootloader، مما يجعل تثبيت أنظمة بديلة مستحيلاً.

2. هواتف الخصوصية المجهزة مسبقاً:

هناك شركات تبيع الهواتف والنظام مثبت عليها جاهزاً:

- **شركة Purism:** لبيع هاتف Librem 5. يتم الشراء مباشرة عبر موقعهم (puri.sm). الشحن عالمي ولكن قد يستغرق وقتاً طويلاً.
- **شركة Pine64:** لبيع هاتف PinePhone. متوفر عبر موقعهم الرسمي (pine64.org).
- **متجر NitroKey:** شركة ألمانية شهيرة تبيع هواتف NitroPhone (وهي أجهزة Pixel محملة بـ GrapheneOS مع تعديلات أمنية إضافية). ميزة هذا الخيار هو الدعم الفني وضمان التثبيت الصحيح.

3. هواتف الأمان العسكري (مثل Bittium):

- تُباع غالباً عبر وكلاء متخصصين للأمن والدفاع، ولكن يمكن العثور عليها أحياناً في متاجر التقنية المتقدمة المتخصصة في الخصوصية (مثل متاجر "Privacy-Focused Tech Stores" في أوروبا أو دبي).

ثالثاً: نصائح عند الشراء والتجهيز:

- **الدفع بخصوصية:** إذا كنت تطلب هاتفاً متخصصاً من الخارج، يفضل البعض استخدام بطاقات دفع "مسبقة الدفع" أو العملات الرقمية (إذا كان المتجر يدعمها) لتقليل ارتباط الجهاز بهويتك البنكية.
- **عنوان الاستلام:** حاول استلام الجهاز في مكان عمل أو عنوان غير مرتبط مباشرة بسكنك الدائم إذا كنت في حالة تهديد أمني عالية.

الرموز التي يمكن كشف اي خلل او اختراق في الموبايل:

تُعرف هذه الرموز تقنياً بـ رموز MMI أو USSD، وهي مخصصة في الأصل لاختبار وظائف الشبكة والجهاز. ورغم أنها لا تكشف برمجيات التجسس المتطورة جداً (مثل بيغاسوس)، إلا أنها فعالة جداً في كشف "تحويل المكالمات" أو التلاعب بإعدادات الشبكة الذي قد تفعله تطبيقات التجسس العادية.

أهم الرموز التي يمكنك تجربتها (تُطلب من لوحة الاتصال كأنك تجري مكالمة):

1. رمز كشف تحويل المكالمات والبيانات (*#62#):

هذا هو الرمز الأهم: إذا كان هناك طرف ثالث يتنصت على مكالماتك عندما يكون هاتفك مغلقاً أو غير متاح، فسيظهر لك الرقم الذي يتم تحويل المكالمات إليه.

ما الذي تبحث عنه: إذا ظهر رقم لا تعرفه (وليس رقم "البريد الصوتي" الخاص بشركتك)، فهذا مؤشر خطر.

2. رمز معرفة حالة التوجيه (*#21#):

يكشف لك: ما إذا كانت الرسائل النصية (SMS)، المكالمات، أو البيانات يتم إعادة توجيهها إلى جهة أخرى دون علمك بشكل "مطلق" (أي حتى والهاتف متاح).

3. رمز إلغاء كافة أنواع التحويل (##002#):

هذا رمز وقائي: إذا شككت في وجود تحويل لمكالماتك أو بياناتك، اطلب هذا الرمز وسيقوم فوراً بتعطيل كافة أنواع "إعادة التوجيه" النشطة على الخط.

4. رمز معرفة الهوية الدولية للجهاز (*#06#):

يظهر لك رقم الـ IMEI: وكالات الاستخبارات تتبع الجهاز عبر هذا الرقم وليس فقط عبر الشريحة.

نصيحة: قارن الرقم الظاهر على الشاشة بالرقم الموجود على علبة الهاتف؛ إذا اختلفا، فهذا يعني أن نظام التشغيل قد تم التلاعب به.

5. رموز اختبار وظائف العتاد (Hardware Test):

تستخدم للتأكد من أن الكاميرا أو الميكروفون لا يعملان بشكل مستقل أو بهما خلل:

- للأندرويد (غالباً سامسونج): *#0*# (يفتح قائمة اختبار الشاشة، الكاميرا، والحساسات دون ضغط اتصال).
- لهواتف أخرى: *#*#4636#*#* (يعطيك معلومات تفصيلية عن الشبكة واستخدام التطبيقات للبيانات).

> **تنبيه هام جداً:**
> هذه الرموز تكشف "اختراق الشبكة" أو تحويل المكالمات التقليدي. أما برمجيات التجسس الاستخباراتية (Spyware) التي تخترق "نظام التشغيل" (مثل تلك التي ناقشناها سابقاً)، فهي لا تستخدم ميزة "تحويل المكالمات" بل تسحب البيانات مباشرة عبر الإنترنت، ولذلك لن تظهر باستخدام هذه الرموز.

كيفية التأكد من أن رقم البريد الصوتي الذي يظهر لك في الرموز هو رقم حقيقي تابع لشركة الاتصالات وليس رقماً مخترقاً؟

للتأكد من أن الرقم الذي يظهر لك هو رقم "البريد الصوتي" الرسمي وليس رقماً مجهولاً يتجسس عليك، اتبع الخطوات البسيطة الآتية:

1. المطابقة عبر الإنترنت (الطريقة الأسرع):

قم بالبحث في جوجل عن: "رقم البريد الصوتي + [اسم شركة اتصالاتك]". شركات الاتصالات تنشر أرقام الخدمة الخاصة بها علنًا. إذا كان الرقم الذي ظهر لك بعد طلب الكود (*#62#) مطابقاً تماماً للرقم المعلن عنه، فأنت في أمان.

2. الاتصال المباشر بالرقم:

قم بالاتصال بالرقم الذي ظهر لك في كود التحويل:

- إذا كان رسمياً: ستسمع الرد الآلي المعتاد لشركة الاتصالات (مثلاً: "مرحباً بك في خدمة البريد الصوتي").
- إذا كان اختراقاً: قد تسمع صوتاً غريباً، أو نغمة اتصال طويلة دون رد، أو يتم فصل المكالمة فوراً.

3. ميزة "حالة الاتصال" في الإعدادات:

يمكنك التأكد من داخل نظام الهاتف نفسه:

- في الأندرويد: اذهب إلى تطبيق الهاتف -> الإعدادات -> البريد الصوتي (Voicemail). ستجد الرقم المسجل هناك، ويمكنك مقارنته بالرقم الذي ظهر لك في الكود.
- في الآيفون: اذهب إلى الإعدادات -> الهاتف -> البريد الصوتي.

ماذا تفعل إذا وجدت رقماً مجهولاً؟

إذا ظهر لك رقم مختلف تماماً ولا ينتمي لشركتك، فقم بالآتي فوراً:

1. **اطلب الكود ##002#:** هذا الكود العالمي سيمسح جميع أرقام التحويل "المزروعة" على خطك فوراً.
2. **تواصل مع الشركة:** اتصل بخدمة العملاء واطلب منهم التأكد من حالة "إعادة توجيه المكالمات" (Call Forwarding) على خطك وإلغائها من جانبهم.
3. **تغيير كلمة مرور البريد الصوتي:** بعض المخترقين لا يحتاجون لاختراق الهاتف، بل يخترقون "صندوق البريد الصوتي" نفسه لسحب رسائلك.

نصيحة إضافية: في بعض الأحيان، يظهر لك رقم يبدو غريباً ولكنه يكون تابعاً للشركة "لأغراض تقنية" (مثل الربط بين خدمات الجيل الرابع والخامس). لذا، التأكد عبر الموقع الرسمي للشركة هو دائماً الفيصل.

هجوم **"تبديل الشريحة" (SIM Swapping):**

هجوم "تبديل الشريحة" (SIM Swapping) هو أحد أخطر الأساليب الاستخباراتية والإجرامية، لأنه يعتمد على اختراق "خطك" لدى شركة الاتصالات وليس اختراق جهازك نفسه. بمجرد نجاح المهاجم في نقل رقمك إلى شريحة يمتلكها، ستتوقف شريحتك عن العمل، وتصل إليه جميع رسائل التحقق (SMS) الخاصة بحساباتك البنكية ومنصات التواصل. وهي طريقة شائعة تستخدمها جهات الاختراق للسيطرة على حساباتك دون لمس هاتفك.

إليك كيف تحمي نفسك من هذا التهديد بفعالية:

1. وضع "رمز PIN" للشريحة (SIM PIN): هذا هو خط الدفاع الأول والمنسي.

- **الوظيفة:** يطلب الهاتف رمزًا سريًا في كل مرة يتم فيها إعادة تشغيل الجهاز أو نقل الشريحة لهاتف آخر.
- **كيفية التفعيل:** اذهب إلى إعدادات الأمان > قفل بطاقة SIM. (تأكد من معرفة الرمز الافتراضي لشركتك، وعادة ما يكون 0000 أو 1234، ثم غيّره لرمز خاص بك).

2. تفعيل "قفل الحماية" لدى شركة الاتصالات: بعض شركات الاتصالات توفر ميزة تسمى " Port Freeze" أو "Account Lock".

- **الوظيفة:** تمنع هذه الخاصية الموظفين من نقل رقمك إلى شريحة جديدة إلا إذا حضرت شخصياً إلى الفرع ومعك هويتك الأصلية، أو قمت بإدخال رمز سري خاص بحسابك لدى الشركة.
- **الإجراء:** اتصل بخدمة العملاء واسألهم: "هل يمكنني وضع قفل حماية لمنع نقل شريحتي إلا بكلمة سر؟".

3. استبدال الرسائل النصية (SMS) بتطبيقات المصادقة: هذا هو الإجراء الأهم للأمان الرقمي:

- **المشكلة:** الرسائل النصية (SMS) غير آمنة وسهلة الاعتراض عبر تبديل الشريحة.
- **الحل:** في إعدادات الأمان لكل حساباتك (جوجل، فيسبوك، واتساب)، اختر "المصادقة الثنائية" عبر تطبيق مثل Google Authenticator أو Authy أو Microsoft Authenticator. هذه الرموز تُولد داخل جهازك ولا ترتبط بشريحة الهاتف.

4. استخدام مفاتيح الأمان الفيزيائية (YubiKey): للمستهدفين بشكل عالي (صحفيين، مسؤولين، نشطاء):

- هذا المفتاح هو قطعة هاردوير صغيرة توضع في منفذ الهاتف أو الكمبيوتر. بدون وجود هذا المفتاح "مادياً" في يدك، لن يفتح الحساب حتى لو امتلك المهاجم رقم هاتفك وكلمة سرك.

5. تقليل نشر معلوماتك الشخصية:

- المهاجم يحتاج لإقناع موظف شركة الاتصالات بأنه "أنت". يقوم بذلك عبر جمع معلوماتك (تاريخ ميلادك، اسم الأم، العنوان) من منشوراتك على وسائل التواصل.

نصيحة: اجعل إجابات "أسئلة الأمان" لدى الشركات وهمية وغير قابلة للتخمين.

علامة التحذير الوحيدة: إذا وجد هاتفك فجأة مكتوباً عليه "No Service" أو "**شريحة غير صالحة**" وأنت في مكان به تغطية، فمن المحتمل جداً أن عملية "تبديل شريحة" قد حدثت الآن. **التصرف الفوري:** استخدم أي هاتف آخر واتصل بشركة الاتصالات فوراً لإيقاف الخط وإبلاغهم أنك لم تطلب تبديل الشريحة.

دور حقيبة او صندوق فارادي في عزل الموبايل عن التتبع:

تعد **حقيبة أو صندوق فارادي (Faraday Bag/Box)** أقوى وسيلة "مادية" لعزل الهاتف تماماً عن العالم الخارجي، ودورها باختصار هو تحويل هاتفك إلى **"ثقب أسود" رقمي.**

تاليا، الدور الذي تلعبه في الحماية من التتبع الاستخباراتي:

1. حجب جميع الإشارات اللاسلكية (Signal Blocking):

تُبطن هذه الحقائب بطبقات من ألياف معدنية موصلة (مثل النحاس أو النيكل). عندما تضع الهاتف داخلها، فإنها تنشئ درعاً يمنع دخول أو خروج أي موجات كهرومغناطيسية. هذا يعني حجب:

- **إشارات الأبراج (Cellular):** لا يمكن للهاتف استقبال مكالمات أو رسائل، ولا يمكن للبرج تحديد موقعك.
- **نظام تحديد المواقع (GPS):** يتم قطع الاتصال بالأقمار الاصطناعية، مما يمنع تسجيل إحداثيات موقعك.
- **الواي فاي والبلوتوث:** يمنع تتبعك عبر نقاط الواي فاي العامة أو أجهزة البلوتوث المحيطة.

2. منع التتبع السلبي (Passive Tracking):

حتى لو قمت بإغلاق الهاتف برمجياً (Power Off)، فإن بعض برمجيات التجسس المتطورة (مثل "بيغاسوس") لديها القدرة على إبقاء الهاتف في حالة "شبه عمل" لإرسال إشارات خفية أو تسجيل الصوت. حقيبة فارادي **تقتل** هذه الإمكانية فيزيائياً لأن الإشارة لن تستطيع اختراق الدرع المعدني مهما كانت قوة البرنامج.

3. الحماية من "الاستنساخ اللاسلكي" (RFID Blocking):

- تمنع الحقيبة القراصنة أو أجهزة الاستخبارات القريبة من استخدام أجهزة مسح لاسلكية لسحب البيانات من شريحة الهاتف أو البطاقات البنكية (NFC) الموجودة بجواره.

متى يستخدمها المحترفون؟

- **أثناء الاجتماعات الحساسة:** لمنع تسجيل الصوت أو تحويل الهاتف لميكروفون تجسس عن بُعد.
- **عند السفر أو التنقل:** لمنع رسم خريطة لتحركاتك عبر أبراج الاتصالات.
- **بعد الشك في الاختراق:** لعزل الجهاز فوراً ومنعه من تسريب البيانات لحين فحصه.

تنبيهات هامة:

- **الجودة:** ليست كل الحقائب متساوية؛ الحقائب الرخيصة قد تسرب إشارة (يمكنك اختبارها بوضع الهاتف داخلها والاتصال به من هاتف آخر، إذا رنّ الهاتف فهي غير صالحة).
- **الاستنزاف:** عند وضع الهاتف داخلها وهو يعمل، سيحاول الجهاز البحث عن شبكة بأقصى طاقة له، مما قد يؤدي لارتفاع حرارته ونفاذ البطارية بسرعة؛ لذا يُفضل إغلاق الهاتف أو تفعيل وضع الطيران قبل وضعه في الحقيبة.

كيفية صنع نسخة منزلية بسيطة من "درع فارادي" باستخدام أدوات مطبخ عادية لاختبار الفكرة:

يمكن صنع نسخة منزلية بسيطة جداً لاختبار المبدأ العلمي لـ "قفص فارادي" باستخدام ورق الألومنيوم (القصدير) العادي المتوفر في المطبخ.

الأدوات المطلوبة:

1. ورق ألومنيوم (قصدير).
2. هاتفك المحمول (وهاتف آخر للاتصال به واختباره).
3. قطعة قماش أو منديل ورقي (اختياري، لمنع خدش الهاتف).

الخطوات:

1. **التحضير:** لفه بمنديل ورقي أولاً (ليكون عازلاً بين جسم الهاتف ومعدن الألومنيوم، ولحماية الشاشة).
2. **التغليف:** قم بلف الهاتف بـ 3 إلى 4 طبقات من ورق الألومنيوم. تأكد من تغطيته بالكامل دون وجود أي ثغرات أو فتحات ولو صغيرة جداً.
3. **الإحكام:** اضغط على الحواف جيداً لضمان عدم تسرب أي موجات كهرومغناطيسية.

كيف تختبر نجاح التجربة؟

4. **استخدم هاتفاً آخر للاتصال برقمك.**

- **النتيجة الناجحة:** يجب أن تسمع رسالة "الهاتف الذي طلبته مغلق أو خارج نطاق الخدمة" فوراً، ولن يرن الهاتف الموجود داخل القصدير إطلاقاً.
- **النتيجة الفاشلة:** إذا رن الهاتف، فهذا يعني أن الطبقات غير كافية أو أن هناك "ثقباً" في التغليف سمح بمرور الموجات.

لماذا ينجح هذا؟

- الألومنيوم مادة موصلة للكهرباء. عندما تصطدم موجات الراديو (إشارة الجوال) برقائق الألومنيوم، تتوزع الشحنات الكهربائية على السطح الخارجي للمعدن وتلغي بعضها البعض في الداخل، مما يجعل الحيز الداخلي صفراً من حيث الإشارات اللاسلكية.

ملاحظات هامة:

- لا تترك الهاتف لفترة طويلة: كما ذكرت لك، الهاتف سيبذل جهداً مضاعفاً للبحث عن الشبكة، مما قد يسخنه بشدة.

- الاستخدام الدائم: هذه الطريقة للاختبار فقط. للاستخدام اليومي، يفضل شراء حقيبة فارادي جاهزة لأنها مصممة من ألياف كربونية ونحاسية تدوم طويلاً ولا تمزق مثل ورق الألومنيوم.

أفضل العلامات التجارية الموثوقة التي تصنع حقائب فارادي احترافية (دولية تشحن، وأخرى متوفرة في تركيا).

تتوفر حقائب فارادي بخيارات متنوعة، بدءاً من الماركات العالمية الرائدة المستخدمة من قبل الوكالات الأمنية، وصولاً إلى خيارات متاحة محلياً في تركيا عبر منصات التجارة الإلكترونية.

أولاً: أفضل الماركات العالمية (تشحن دولياً):

تُعد هذه الشركات "المعيار الذهبي" في عزل الإشارات، وتستخدمها وحدات إنفاذ القانون والجيوش عالمياً:

- **Mission Darkness (تتبع شركة MOS Equipment):**
  - ❖ لماذا يفضلها الخبراء؟: تُصنف كأفضل الماركات الشاملة (Best Overall). تستخدم تقنيات حجب عسكرية وتوفر حقائب لكل شيء من المفاتيح إلى الحواسيب المحمولة.
  - ❖ أشهر منتجاتها: Non-Window Faraday Bag للهواتف.
- **SLNT (Silent Pocket سابقاً):**
  - ❖ لماذا يفضلها الخبراء؟: تتميز بتصميمات أنيقة (مثل الجلد) لا تبدو كحقائب تقنية، وتستخدم تقنية "Silent Pocket Cage" الحاصلة على براءة اختراع.
  - ❖ أشهر منتجاتها: Faraday Phone Sleeve.
- **GoDark:**
  - ❖ لماذا يفضلها الخبراء؟: تركز على المتانة الشديدة (Rugged) ومقاومة الماء، وهي مفضلة لمحبي الرحلات والعمل الميداني.
- **OffGrid (تتبع شركة EDEC):**
  - ❖ لماذا يفضلها الخبراء؟: معروفة بجودة التصنيع العالية وتستخدم بكثرة في التحقيقات الجنائية الرقمية.

ثانياً: الأنواع المتوفرة في تركيا (شراء محلي):

يمكنك العثور على حقائب فارادي في السوق التركي عبر المنصات الكبرى، وغالباً ما تكون تحت أسماء تقنية مثل "Sinyal Kesici Kılıf" أو "Faraday Çantası":

- **Hepsiburada & Amazon Turkey:**
  - ❖ تتوفر ماركات مثل LMLXYZ و Simket (وهي خيارات اقتصادية فعالة تم اختبارها بنجاح لحجب إشارات الجوال والمفاتيح).
- **Ubuy Turkey:**
  - ❖ يوفر هذا الموقع إمكانية طلب الماركات العالمية (مثل Mission Darkness و SLNT) من الخارج وشحنها مباشرة إلى تركيا مع دفع الرسوم الجمركية مسبقاً.
- **SuperKilometerFilter (SKF):**
  - ❖ يوفر حقائب متخصصة في تركيا تركز بشكل أساسي على حماية مفاتيح السيارات من السرقة الرقمية، ولكنها تعمل بفعالية للهواتف أيضاً.

ثالثاً: معايير اختيار الحقيبة المناسبة:

عند الشراء، تأكد من الآتي لضمان أعلى مستوى من الخصوصية:

1. **عدد الطبقات:** ابحث عن الحقائب ذات "الطبقات المزدوجة" (Dual-layer) أو الثلاثية لضمان عدم تسرب إشارات G5 القوية.
2. **نوع القماش:** الألياف التي تحتوي على النحاس والنيكل هي الأكثر كفاءة في الحجب.
3. **طريقة الإغلاق:** يفضل نظام "اللف" (Roll-top) أو الإغلاق المغناطيسي المزدوج لضمان عدم وجود أي فجوة يمر منها التردد.

كيفية اختبار جودة الحقيبة فور وصولها إليك للتأكد من أنها ليست مجرد قماش عادي؟

لاختبار حقيبة فارادي والتأكد من أنها توفر حماية حقيقية وليست مجرد قطعة قماش عادية، اتبع الاختبارات الثلاثة التالية بالترتيب:

1. اختبار الاتصال (الأبسط):

- ضع الهاتف داخل الحقيبة وأغلقها بإحكام حسب تعليمات المصنع.
- انتظر لمدة 30 ثانية (ليقوم الهاتف بمحاولة البحث عن شبكة ثم اليأس منها).
- اتصل بهاتفك من هاتف آخر.
- النتيجة السليمة: يجب أن تسمع رسالة "الهاتف مغلق أو خارج نطاق التغطية" فوراً. إذا رن الهاتف، فالحقيبة لا تحجب إشارات الأبراج (Cellular).

2. اختبار الواي فاي والبلوتوث (الأكثر دقة):

إشارات الواي فاي والبلوتوث تعمل بترددات مختلفة (2.4 و 5 جيجاهرتز) وهي أصعب في الحجب:

- قبل وضع الهاتف في الحقيبة، اتصل بشبكة واي فاي وافتح مكبر صوت بلوتوث أو اربط ساعة ذكية.
- ضع الهاتف في الحقيبة وأغلقها.
- راقب الأجهزة المرتبطة؛ إذا انقطع اتصال الساعة الذكية أو توقفت الموسيقى في مكبر الصوت فوراً، فهذا دليل على جودة العزل.
- حاول البحث عن موقع الهاتف عبر خدمة "**Find My Device**" من كمبيوتر؛ إذا لم يستطع تحديد الموقع، فالعزل ممتاز.

3. استخدام تطبيقات قياس الإشارة (للمحترفين):

إذا أردت دليلاً رقمياً، يمكنك تحميل تطبيقات مثل **Network Cell Info Lite** أو **WiFi Analyzer**:

- افتح التطبيق وشاهد قوة الإشارة (ستكون مثلاً ‎-70 dBm‎).
- ضع الهاتف في الحقيبة (اترك سحاباً صغيراً مفتوحاً لتراقب الشاشة للحظة ثم أغلقه تماماً).
- يجب أن تنخفض الإشارة إلى "**لا توجد خدمة**" أو يظهر رقم ضعيف جداً (مثل ‎-110 dBm‎ أو أقل) قبل أن تختفي تماماً.

4. اختبار "المصباح" (كشف الثغرات المادية):

- في غرفة مظلمة، ضع مصباحاً قوياً (Flashlight) داخل الحقيبة وأغلقها.
- إذا رأيت أي تسرب للضوء من الخياطة أو الزوايا، فهذا يعني أن موجات الراديو (التي هي أصغر من موجات الضوء) يمكنها التسرب أيضاً. الحقيبة الاحترافية يجب أن تكون "كتيمة" تماماً للضوء.

نصيحة أخيرة:

بمرور الوقت، قد تتآكل الألياف المعدنية داخل الحقيبة بسبب كثرة الثني. كرر اختبار الاتصال **مرة كل شهر** للتأكد من أن الحقيبة لا تزال تعمل بكفاءة.

الأخطاء الشائعة التي يقع فيها المستخدمون وتؤدي لفشل عزل الحقيبة، مثل طريقة الطي أو تداخل الأجهزة:

يقع الكثيرون في أخطاء بسيطة تجعل أقوى حقيبة فارادي عديمة الفائدة. تاليا أبرز هذه الأخطاء وكيف يمكن تجنبها لضمان العزل التام:

1. الخطأ في طريقة "الطي" (The Roll):

معظم الحقائب الاحترافية تعتمد على نظام "**الطي واللف**" **(Roll-top)** وليس السحاب فقط.

- **الخطأ:** إغلاق اللاصق (Velcro) فقط دون لف حافة الحقيبة.
- **الصواب:** يجب لف الحافة العلوية مرتين أو ثلاث مرات على الأقل قبل إغلاق المشبك. هذا يضمن تداخل الألياف المعدنية ومنع تسرب الموجات من الفتحة.

2. تداخل الأجهزة (Device Crowding):

- **الخطأ:** وضع أكثر من هاتف داخل حقيبة واحدة صغيرة، أو وضع الهاتف بجانب مفاتيح السيارة أو بطاقات بنكية.
- **السبب:** عندما تلمس الأجهزة بعضها أو تضغط على جدران الحقيبة، قد تؤدي البروزات (مثل أزرار الهاتف) إلى إحداث فجوات ميكروبية في الدرع المعدني، مما يسمح للإشارة بالمرور.
- الصواب: اترك مساحة بسيطة داخل الحقيبة، ولا تجعلها "مشدودة" لدرجة تمدد الألياف.

3. وجود أوساخ أو زيوت على الحواف:

- **الخطأ:** ملامسة الحواف الداخلية للحقيبة بأيدي ملوثة بالزيوت أو الأتربة.
- **السبب:** المواد العازلة تعتمد على "التوصيل الكهربائي" التام بين الألياف. الزيوت والأوساخ تعمل كعازل يمنع التلامس الكامل للألياف عند الإغلاق، مما يخلق ثغرة إلكترونية.

4. وضع الهاتف وهو في حالة "نشاط مكثف":

- **الخطأ:** وضع الهاتف داخل الحقيبة أثناء تحميل ملف كبير أو تحديث نظام.
- **السبب:** هذا يؤدي لارتفاع حرارة الهاتف بشكل خطير لأن الحقيبة تعزل الحرارة أيضاً. الحرارة الزائدة قد تتلف بطارية الهاتف أو تؤدي لتآكل الطبقة الداخلية للحقيبة.
- **الصواب:** أغلق التطبيقات الثقيلة أو فعل "وضع الطيران" قبل وضعه في الحقيبة إذا كنت ستبقيه هناك لفترة طويلة.

5. إهمال "تآكل" البطانة الداخلية:

- **الخطأ:** ثني الحقيبة ووضعها في الجيب الخلفي أو الجلوس عليها.
- **السبب:** بطانة فارادي مصنوعة من أنسجة معدنية رقيقة جداً. كثرة الثني العنيف تؤدي لتكسر هذه الألياف، ومع الوقت تظهر "ثقوب" غير مرئية تمر منها موجات الـ G5 والـ Wi-Fi.

6. استخدام "نظام النافذة" بشكل خاطئ:

بعض الحقائب بها نافذة شفافة لرؤية الشاشة:

- **الخطأ:** خدش هذه النافذة أو وضع أجسام حادة بجانبها. هذه النافذة هي أضعف نقطة في الحقيبة، وأي تلف بسيط فيها يعني ضياع العزل تماماً.

نصيحة احترافية: إذا كنت تريد التأكد من أنك لست "مراقبًا بالصوت" حتى داخل الحقيبة، يفضل وضع الهاتف داخل "كم سيلكون" سميك قبل وضعه في حقيبة فارادي؛ فالسيليكون يمتص الاهتزازات الصوتية ويصعب مأمورية الميكروفونات الحساسة.

كيفية تنظيف الحقيبة دون إتلاف الألياف المعدنية الحساسة بداخلها:

تخزين حقيبة فارادي بشكل صحيح هو ما يحدد عمرها الافتراضي، لأن الألياف المعدنية بداخلها حساسة جداً للانثناءات المتكررة. إليك الطريقة المثالية لتخزينها:

1-وضعية "التسطيح (Lay it Flat)":

القاعدة الأهم: لا تقم بطي الحقيبة أو ثنيها عند عدم الاستخدام.

- الطريقة: احفظها في وضعية مفرودة (مسطحة) داخل درج أو على رف. ثني الحقيبة وهي فارغة يؤدي إلى تكسير الألياف المعدنية في زوايا الثني، مما يخلق ثغرات تسمح بمرور الإشارة مستقبلاً.

2-الحماية من الرطوبة:

- الألياف الداخلية (غالباً من النحاس والنيكل) تتأثر بالرطوبة وتتعرض لـ الأكسدة، مما يفقدها قدرتها على العزل.
- نصيحة: ضع الحقيبة في مكان جاف، ويفضل وضع كيس صغير من "هلام السيليكا (Silica Gel) " –تلك الأكياس الصغيرة التي تجدها في صناديق الأحذية – داخل الحقيبة أو بجانبها لامتصاص أي رطوبة.

3- الابتعاد عن الأجسام الحادة:

- لا تخزن الحقيبة في مكان يحتوي على مفاتيح أو أدوات حادة قد تثقب البطانة الداخلية. أي ثقب، ولو بحجم رأس الإبرة، قد يقلل من كفاءة حجب إشارات التردد العالي) مثل G.5

4-تجنب الضغط الثقيل:

- لا تضع كتباً ثقيلة أو أغراضاً فوق الحقيبة أثناء تخزينها، لأن الضغط المستمر يضعف نسيج العزل ويقلل من مرونته.

5- إغلاق خفيف:

- عند التخزين، لا تقم بلف الحافة (Roll) بإحكام كما تفعل عند وضع الهاتف. اتركها مفتوحة أو مغلقة بشكل بسيط جداً لتجنب إجهاد نقاط الطي.

نصيحة أخيرة: إذا كنت تمتلك أكثر من حقيبة، لا تضعها فوق بعضها البعض بشكل متراص جداً، بل اترك مساحة تسمح بمرور الهواء لمنع تراكم الرطوبة بينها.

لمعرفة كيفية تشفير ملفاتك الحساسة داخل الهاتف بحيث حتى لو تم الوصول للجهاز لا يمكن قراءتها؟

تشفير الملفات هو "خط الدفاع الأخير"؛ فإذا نجح المخترق في الوصول إلى جهازك، سيجد بياناتك عبارة عن رموز غير مفهومة لا يمكن قراءتها بدون مفتاح التشفير الخاص بك.

إليك أفضل الطرق لتشفير ملفاتك الحساسة على الهواتف الذكية:

1. استخدام "المجلد الآمن" المدمج (للمستخدم العادي)

أغلب الهواتف الحديثة توفر نظام تشفير مدمج يعزل ملفاتك عن بقية النظام:

- **في سامسونج (Secure Folder)**: يعتمد على تقنية Knox العسكرية. يقوم بتشفير الصور والملفات والتطبيقات بشكل منفصل تماماً، ويتطلب كلمة مرور أو بصمة مختلفة عن قفل الشاشة.
- **في أندرويد الخام (Locked Folder)**: ميزة داخل "صور جوجل" و"تطبيق الملفات" تتيح لك نقل الصور والوثائق إلى مجلد مشفر لا يظهر في الاستوديو ولا يُنسخ احتياطياً للسحاب إلا بإذنك.
- **في آيفون:** استخدم ميزة "الملاحظات المقفلة" (Locked Notes) لتخزين البيانات الحساسة وتشفيرها ببصمة الوجه، أو ميزة "المجلد المخفي" في الصور الذي يتطلب FaceID.

2. تطبيقات التشفير الاحترافية (لأقصى حماية):

إذا كنت تريد تشفيراً لا يعتمد على نظام تشغيل الهاتف (خوفاً من وجود ثغرة في النظام نفسه)، استخدم تطبيقات مستقلة تستخدم خوارزميات مثل **AES-256**:

- **Cryptomator (الأفضل للخصوصية)**: تطبيق مفتوح المصدر يقوم بتشفير ملفاتك قبل رفعها لأي خدمة سحابية. حتى لو اخترق شخص حسابك في Google Drive، سيجد ملفات مشفرة لا يمكن فتحها إلا عبر التطبيق بمفتاحك الخاص.
- **EDS (Encrypted Data Store)**: مخصص للأندرويد، يتيح لك إنشاء "حاويات" مشفرة (Containers) تشبه الخزنة، ولا يمكن لأي تطبيق آخر في الهاتف رؤية ما بداخلها.
- **VeraCrypt (للحواسيب)**: إذا كنت تنقل ملفات من الكمبيوتر للهاتف، استخدمه لإنشاء أقراص وهمية مشفرة.

نصائح حاسمة عند التشفير:

- **كلمة مرور قوية ومستقلة:** لا تستخدم نفس كلمة مرور قفل الشاشة للمجلد المشفر. إذا عرف المخترق الأولى، ستسقط الثانية تلقائياً.
- **تجنب النسخ الاحتياطي السحابي التلقائي:** تأكد من استثناء "المجلد المشفر" من النسخ الاحتياطي التلقائي لـ (iCloud أو Google Photos) إلا إذا كنت تستخدم تطبيقاً مثل Cryptomator الذي يشفرها قبل الرفع.
- **احذر من ضياع كلمة المرور:** في أنظمة التشفير القوية، لا يوجد خيار "نسيت كلمة المرور". إذا فقدت الرمز، ستفقد ملفاتك للأبد لأنه لا توجد "أبواب خلفية".

4. ميزة "تشفير الجهاز بالكامل" (Full Disk Encryption):

تأكد من إعدادات الهاتف أن ميزة "تشفير الهاتف" مفعلة (غالباً ما تكون مفعلة تلقائياً في الأنظمة الحديثة بمجرد وضع قفل للشاشة). هذا يمنع استخراج البيانات من ذاكرة الهاتف في حال تم توصيله بجهاز كمبيوتر خارجي وهو مغلق.

كيفية إدارة كلمات المرور المعقدة لهذه المجلدات والحسابات باستخدام مدير كلمات مرور (Password Manager) آمن وغير قابل للاختراق؟

إدارة كلمات المرور هي "المفتاح" لكل دفاعاتك الرقمية. استخدام كلمة مرور واحدة لكل شيء هو خطأ أمني فادح، لذا فإن **مدير كلمات المرور (Password Manager)** هو الأداة التي ستقوم بإنشاء وتخزين كلمات مرور فريدة ومعقدة لكل حساب، بحيث لا تحتاج سوى لحفظ "كلمة مرور رئيسية" واحدة قوية جداً.

إليك أفضل الأدوات وكيفية استخدامها بأمان:

1. أفضل مديري كلمات المرور (الأكثر أماناً):

- **Bitwarden (الأكثر ترشيحاً):** هو الخيار المفضل لخبراء الخصوصية لأنه مفتوح المصدر بالكامل، مما يعني أن الكود البرمجي الخاص به مراجع أمنياً من قبل الجميع. يوفر نسخة مجانية ممتازة تتيح لك المزامنة بين هاتفك وكمبيوترك.
- **KeePassXC / KeePassDX:** هذا الخيار للمحترفين الذين يرفضون تخزين بياناتهم على "السحاب". يقوم بتخزين قاعدة بيانات كلمات المرور في ملف محلي على جهازك فقط. أنت المسؤول عن نقل هذا الملف وتأمينه، مما يجعله مستحيلاً على أي جهة استخباراتية اختراقه عن بُعد.
- **Password1:** يتميز بواجهة سهلة جداً وميزات أمنية متقدمة مثل "وضع السفر" (Travel Mode) الذي يحذف كلمات المرور من جهازك مؤقتاً عند عبور الحدود لمنع تفتيشها، ثم يعيدها بمجرد وصولك لوجهتك.

2. قواعد ذهبية لإعداد مدير كلمات المرور

- **كلمة المرور الرئيسية (Master Password):** يجب أن تكون طويلة (أكثر من 15 حرفاً) وتتكون من جملة عشوائية صعبة التخمين لكن سهلة الحفظ (مثلاً: Ana*Mosafer*2026*Fi*Turkey!). إذا ضاعت هذه الكلمة، ستفقد الوصول لكل حساباتك.
- **المصادقة الثنائية (FA2):** يجب تفعيل المصادقة الثنائية على حساب "مدير كلمات المرور" نفسه. يفضل استخدام مفتاح أمان فيزيائي (YubiKey) ليكون هو القفل الوحيد لهذا المخزن.
- **الخروج التلقائي (Auto-Lock):** اضبط التطبيق ليقوم بالقفل التلقائي بعد دقيقة واحدة من عدم الاستخدام أو عند إغلاق الشاشة.

3. تجنب "مدير كلمات المرور" في المتصفح:

- **تحذير:** تجنب حفظ كلمات المرور الحساسة داخل متصفحات مثل Chrome أو Edge. هذه المتصفحات ليست مخصصة للأمان العالي، وهناك برمجيات تجسس بسيطة (Infostealers) مصممة خصيصاً لسحب كلمات المرور المخزنة في المتصفحات بمجرد اختراق الجهاز.

4. ميزة "مولد كلمات المرور" (Generator):

استخدم المولد الموجود داخل التطبيق لإنشاء كلمات مرور عشوائية مثل (x9#K2p!Lz@8vQ). لا تحاول ابتكارها بنفسك؛ فالعقل البشري يميل لأنماط يمكن للذكاء الاصطناعي الاستخباراتي تخمينها بسرعة.

نصيحة أخيرة: قم بطباعة "كود الطوارئ" (Emergency Kit) الذي يعطيه لك التطبيق عند التسجيل، وضعه في مكان مادي آمن (مثل خزنة منزلية) بعيداً عن أي جهاز إلكتروني.

كيف تكتشف إذا كانت بياناتك أو كلمات مرورك قد سُربت بالفعل في الماضي على الإنترنت المظلم (Dark Web)؟

تاليا، الطريقة الأكثر فاعلية للكشف عن تسريب بياناتك في "الإنترنت المظلم" (Dark Web)، وهي خطوة ضرورية لأنك قد تكون مخترقاً "رقمياً" منذ سنوات دون أن تدري:

1. موقع Have I Been Pwned (الأكثر ثقة عالمياً):

هذا الموقع هو المرجع الأول للخبراء. يقوم بجمع بيانات مليارات الحسابات المسربة من الاختراقات الكبرى (مثل اختراقات فيسبوك، لينكد إن، وغيرها).

- **كيفية الاستخدام:** ادخل إلى haveibeenpwned.com واكتب بريدك الإلكتروني أو رقم هاتفك (بصيغة دولية).
- **النتائج:**
  - ❖ **باللون الأخضر:** بياناتك لم تظهر في التسريبات المعروفة.
  - ❖ **باللون الأحمر:** بياناتك سُربت! سيعطيك الموقع قائمة بالمواقع التي سُربت بياناتك منها، وما هي المعلومات التي كُشفت (كلمة مرور، عنوان، تاريخ ميلاد).

2. ميزة "فحص الأمان" في جوجل وآبل:

- **جوجل (Google One):** يوفر لمشتركيه ميزة "Dark Web Report" التي تبحث عن بريدك في المواقع المشبوهة وتنبيهك فور ظهور أي معلومة تخصك.
- **آيفون (Passcodes):** إذا ذهبت إلى الإعدادات > كلمات السر، سيظهر لك تنبيه بجانب كلمات السر التي ظهرت في تسريبات أمنية، ويطلب منك تغييرها فوراً.

3. متصفح Firefox Monitor:

خدمة مجانية من شركة موزيلا (Firefox) تقوم بإرسال تنبيه فوري لبريدك الإلكتروني في حال حدوث اختراق جديد لموقع أنت مسجل فيه، مما يسمح لك بتغيير كلمة المرور قبل أن يستغلها المخترقون.

4. ماذا تفعل إذا وجدت بياناتك مسربة؟

لا داعي للذعر، ولكن تحرك بسرعة:

1. **تغيير كلمة المرور فوراً:** للموقع الذي تم اختراقه، ولكل المواقع الأخرى التي تستخدم فيها نفس كلمة المرور (هنا تبرز أهمية مدير كلمات المرور الذي ناقشناه).
2. **تفعيل المصادقة الثنائية (FA2):** حتى لو امتلك المخترق كلمة السر المسربة، لن يستطيع دخول حسابك بدون رمز التحقق الثاني.
3. **الحذر من رسائل التصيد:** غالباً ما يستخدم المخترقون البيانات المسربة (مثل اسمك وهاتفك) لإرسال رسائل بريد إلكتروني تبدو رسمية لإقناعك بالضغط على روابط خبيثة.

5. تنبيه بخصوص أرقام الهواتف:

إذا سُرب رقم هاتفك، فقد تلاحظ زيادة في المكالمات العشوائية أو رسائل "السبام". في هذه الحالة، يفضل استخدام تطبيقات مثل **Truecaller** بحذر، أو تفعيل خاصية "حجب المتصلين المجهولين" في هاتفك.

دليل الأمان الرقمي الشامل (Checklist) الذي يلخص كل ما تم ذكره سابقا، مرتباً من الإجراءات الفورية إلى الوقاية طويلة الأمد، لضمان أعلى مستويات الخصوصية في مواجهة التتبع الاستخباراتي:

1. الإجراءات الفورية لتأمين الهاتف:

- **إعادة التشغيل اليومي:** لقطع اتصال برمجيات التجسس التي تعيش في الذاكرة المؤقتة.
- **تفعيل وضع الإغلاق (Lockdown Mode):** لمستخدمي آيفون (iOS 16 فأحدث).
- **تحديث النظام والتطبيقات:** سد الثغرات (Zero-day) فور صدور تحديثاتها.
- **مراجعة الأذونات:** سحب صلاحيات الميكروفون والكاميرا والموقع من أي تطبيق غير ضروري.

2. الحماية من التتبع المادي والشبكي:

- **استخدام رموز MMI:** اطلب *#62# للتأكد من عدم وجود تحويل للمكالمات، و##002# لإلغاء أي تحويل نشط.
- **حقيبة فارادي (Faraday Bag):** استخدمها أثناء الاجتماعات الحساسة أو التنقل لعزل الإشارات تماماً.
- **تشفير الـ SIM:** وضع رمز PIN لشريحة الهاتف لمنع هجمات "تبديل الشريحة".
- **إخفاء الـ IP:** تفعيل خاصية "حماية عنوان IP في المكالمات" في واتساب وسيجنال.

3. تأمين الحسابات والبيانات:

- **مدير كلمات المرور (Bitwarden):** لإنشاء وتخزين كلمات مرور معقدة وفريدة لكل حساب.
- **المصادقة الثنائية (FA2):** استخدام تطبيقات (Google Authenticator) والابتعاد عن الرسائل النصية (SMS).
- **تشفير الملفات:** استخدام "المجلد الآمن" أو تطبيقات مثل (Cryptomator) لتشفير الوثائق الحساسة.
- **فحص التسريبات:** التأكد من موقع (Have I Been Pwned) لتغيير كلمات السر المسربة قديماً.

4. للمستويات العليا من الخصوصية (الخيارات المتقدمة):

- **الهواتف المتخصصة:** التفكير في اقتناء جهاز (Google Pixel) وتثبيت نظام (GrapheneOS).
- **تطبيقات المراسلة:** الاعتماد الكلي على تطبيق (Signal) مع تفعيل "الرسائل المختفية".
- **مفاتيح الأمان:** استخدام (YubiKey) كقفل فيزيائي لحسابات البريد الإلكتروني الحساسة.

نصيحة أخيرة: الأمان الرقمي ليس منتجاً تشتريه، بل هو **سلوك يومي**. ابقَ دائماً متشككاً في الروابط الغريبة والمكالمات المجهولة.

دور الذكاء الاصطناعي في التجسس:

دخل الذكاء الاصطناعي (AI) كعنصر حاسم غير قواعد اللعبة في عالم الاستخبارات، حيث نقل التتبع من مجرد "جمع للمعلومات" إلى "تنبؤ بالسلوكيات". لم تعد الوكالات بحاجة لآلاف الموظفين لمراقبة الأهداف، فالخوارزميات تقوم بذلك الآن بدقة مرعبة. تاليا أبرز أدوار الذكاء الاصطناعي في التجسس الحديث:

1. تحليل البيانات الضخمة (Big Data Analytics):

تجمع أجهزة الاستخبارات مليارات البيانات يومياً (مكالمات، رسائل، تحركات). يقوم الذكاء الاصطناعي بـ:

- **تحديد الأنماط:** ربط علاقات بين أشخاص قد لا يبدو بينهم صلة ظاهرة.
- **كشف الشذوذ:** ملاحظة أي تغيير طفيف في سلوك الشخص الرقمي (مثل تغيير مسار الطريق المعتاد أو استخدام كلمات مشفرة جديدة).

2. التعرف على الوجه والصوت المتقدم:

- **المراقبة الحية:** ربط آلاف كاميرات الشوارع بأنظمة ذكاء اصطناعي يمكنها التعرف على "المستهدف" حتى لو كان يرتدي قناعاً أو قام بتغيير ملامحه، عبر تحليل "مشية الشخص" (Gait Recognition) أو هندسة العظام.
- **البصمة الصوتية:** القدرة على عزل صوت المستهدف في مكان مزدحم وتتبعه عبر أي ميكروفون قريب (هاتف، سماعة ذكية).

3. الهجمات السيبرانية الذكية (AI-Powered Cyberattacks):

- **تطوير برمجيات خبيثة ذاتية التطور:** برامج تجسس يمكنها تعديل كودها البرمجي لتجاوز برامج الحماية (Antivirus) تلقائياً دون تدخل بشري.
- **التصيد الاحتيالي المخصص (Spear Phishing):** استخدام الذكاء الاصطناعي لكتابة رسائل بريد إلكتروني تحاكي أسلوب أصدقائك أو زملائك في العمل تماماً لإغرائك بفتح رابط مخترق.

4. التزييف العميق (Deepfakes) في العمليات الاستخباراتية:

- **انتحال الشخصية:** تخليق فيديوهات أو مقاطع صوتية لمسؤولين أو أشخاص مقربين منك لطلب معلومات حساسة أو لإحداث بلبلة سياسية.
- **خلق هويات وهمية:** إنشاء حسابات على التواصل الاجتماعي بوجوه وسير ذاتية وهمية بالكامل للتسلل إلى دوائر اجتماعية معينة وجمع المعلومات.

5. فك التشفير والتنبؤ بالثغرات:

- يُستخدم الذكاء الاصطناعي لتسريع عمليات "كسر التشفير" عبر تجربة ملايين الاحتمالات في ثوانٍ، وأيضاً للبحث عن ثغرات غير مكتشفة في أنظمة التشغيل (Zero-day vulnerabilities) لاستغلالها قبل أن تسدها الشركات.

كيف تحمي نفسك من "التجسس الذكي"؟

- **تقليل البصمة الرقمية:** قلل من نشر صور واضحة لوجهك أو تسجيلات صوتية طويلة على المنصات العامة، لتقليل المواد المتاحة لتدريب "التزييف العميق" عليك.

- **استخدام أدوات الحماية القائمة على AI:** كما يستخدمه المهاجمون، استخدم برامج حماية (مثل تلك التي ناقشناها سابقاً) تستخدم الذكاء الاصطناعي لرصد السلوكيات الخبيثة غير المعروفة.

كيفية كشف التزييف العميق (Deepfake) في المكالمات الفيديوية أو الصوتية إذا تعرضت لمحاولة خداع:

كشف التزييف العميق (Deepfake) في الوقت الفعلي أصبح تحدياً كبيراً، لكن بما أن هذه التقنية تعتمد على معالجة برمجية مكثفة، فإنها لا تزال تترك "آثاراً رقمية" وسلوكية يمكن ملاحظتها إذا كنت منتبهاً.

إليك كيفية كشف التزييف العميق في المكالمات الصوتية والمرئية:

1. في مكالمات الفيديو (Video Deepfakes):

- **اختبار "الجانب" (The Profile Test):** اطلب من الشخص أن يدير وجهه تماماً لليسار أو اليمين. معظم خوارزميات التزييف العميق تفشل في الحفاظ على ملامح الوجه المشوهة عند الانتقال من الوضع الأمامي إلى الجانبي، وستلاحظ "اهتزازاً" أو اختفاءً للملامح عند حافة الوجه.
- **عائق اليد (The Hand Obstruction):** اطلب منه وضع يده أمام وجهه أو المسح على جبهته. الذكاء الاصطناعي يواجه صعوبة في معالجة "التقاطع" بين اليد والوجه، مما يؤدي لظهور تشوهات بصرية (Blur) حول الأصابع.
- **الرمش وحركة العين:** راقب وتيرة رمش العين؛ فأنظمة التزييف العميق غالباً ما تجعل الشخص يرمش بشكل غير طبيعي (إما نادراً جداً أو بكثرة). كما أن انعكاس الضوء داخل العين غالباً ما يكون ثابتاً ولا يتغير مع حركة الرأس.
- **عدم تطابق الصوت مع الشفاه:** ابحث عن تأخير بسيط (Millisecond Delay) بين حركة الفم وخروج الصوت، خاصة عند نطق الحروف التي تتطلب إغلاق الشفاه مثل (ب، م، ف).

2. في المكالمات الصوتية (Audio Deepfakes):

- **نبرة الصوت المعدنية:** غالباً ما يفتقر الصوت المولد بالذكاء الاصطناعي إلى "العواطف البشرية" أو التغيرات المفاجئة في طبقة الصوت عند الانفعال. يبدو الصوت رتيباً أو "مسطحاً".
- **اختبار الأسئلة الشخصية:** إذا شككت في المتصل، اسأله سؤالاً لا يعرف إجابته سوى الشخص الحقيقي (مثلاً: "ماذا أكلنا في آخر مرة التقينا؟"). الذكاء الاصطناعي لا يملك ذاكرة للمواقف الشخصية غير المسجلة رقمياً.
- **الهدوء غير الطبيعي:** في المكالمات الحقيقية، توجد ضوضاء خلفية بسيطة أو صوت أنفاس. الصوت المولد بالذكاء الاصطناعي غالباً ما يكون "نظيفاً" بشكل مبالغ فيه، أو يحتوي على تقطعات رقمية تشبه طنين الكهرباء.

إجراءات وقائية تقنية

- **كلمة السر العائلية:** اتفق مع أفراد عائلتك أو زملائك في العمل على "كلمة سر" شفهية تُستخدم فقط في الحالات الطارئة أو عند الشك في الهوية. إذا لم يستطع الطرف الآخر ذكرها، فهو مزيف.
- **المطالبة بحركة غير متوقعة:** اطلب من الشخص القيام بحركة عشوائية، مثل "المس أنفك بإصبعك السبابة" أو "اقفز". هذه الحركات المفاجئة تكسر معالجة الخوارزمية في الوقت الفعلي وتكشف الخداع.

4. استخدام أدوات الكشف (Deepfake Detectors)

- هناك منصات مثل **Intel's FakeCatcher** أو تطبيقات متخصصة بدأت تظهر في المتاجر، تقوم بتحليل تدفق الدم في الوجه عبر الكاميرا (الذي لا يمكن تزييفه بدقة حتى الآن) لتحديد ما إذا كان الوجه بشرياً حقيقياً أم مولداً.

كيفية استغلال هذه التقنيات في الابتزاز وكيفية التصرف قانونياً وتقنياً في حال وقوع ذلك:

تُستخدم تقنيات التزييف العميق (Deepfake) في الابتزاز عبر تخليق صور أو فيديوهات خادشة أو محرجة للضحية، بهدف الحصول على أموال أو معلومات حساسة. هذا النوع من الهجمات يُعرف بـ "الابتزاز الجنسي الرقمي" (Sextortion) أو "الابتزاز السياسي/ المؤسسي".

إليك كيفية التعامل مع هذا الموقف الحرج من الناحيتين التقنية والقانونية:

أولاً: التصرف الفوري (قاعدة "لا استجابة"):

1. **لا تدفع ولا تتفاوض:** الرضوخ للمبتز يجعله يتمسك بك أكثر ويطلب مبالغ أكبر، كما أن الدفع لا يضمن مسح المحتوى المزيف.
2. **قطع التواصل فوراً:** قم بحظر (Block) المبتز على كافة المنصات، ولا تحاول تبرير أن الفيديو مزيف له؛ هو يعلم ذلك بالفعل.
3. **توثيق الأدلة:** قبل الحظر، قم بأخذ لقطات شاشة (Screenshots) للمحادثات، واسم الحساب، والرابط (URL) الخاص بملفه الشخصي، والرسائل التهديدية.

ثانياً: الإجراءات التقنية لحذف المحتوى:

1. **التبليغ للمنصات:** جميع المنصات الكبرى (فيسبوك، إكس، إنستغرام، يوتيوب) لديها سياسات صارمة ضد "المحتوى الجنسي غير الرضائي" و"التزييف العميق". استخدم خيار "التبليغ عن انتحال شخصية" أو "محتوى غير لائق".
2. **استخدام أداة StopNCII.org:** هي أداة عالمية مدعومة من شركات التقنية، تتيح لك رفع النسخة المزيفة (بشكل مشفر وآمن) لإنشاء بصمة رقمية لها (Hash)، مما يمنع انتشارها أو رفعها مرة أخرى على المنصات المشاركة.
3. **تنبيه المقربين:** في حالات معينة، قد يكون من الأفضل إخبار الدائرة المقربة بأن هناك "فيديو مزيفاً بتقنيات الذكاء الاصطناعي" يتم تداوله، لقطع الطريق على المبتز قبل تواصله معهم.

ثالثاً: التحرك القانوني (خاصة في تركيا):

القانون التركي صارم جداً في جرائم الإنترنت:

- **شرطة الجرائم السايبرانية (Siber Suçlarla Mücadele):** يمكنك التوجه لأقرب مركز شرطة أو تقديم بلاغ عبر بوابة (e-Devlet) أو عبر موقع الأمن العام التركي (Emniyet).
- **قانون العقوبات:** الابتزاز عبر التزييف العميق يندرج تحت مواد "انتهاك خصوصية الحياة الخاصة" و"التهديد والابتزاز"، وتصل عقوباتها للسجن لسنوات.
- **طلب حجب الوصول:** يمكنك عبر محامي تقديم طلب لمحكمة الصلح والجزاء (Sulh Ceza Hakimliği) لاستصدار قرار عاجل بحجب رابط المحتوى المسيء داخل تركيا.

رابعاً: الوقاية من الوقوع ضحية للابتزاز الذكي:

- **فلترة قائمة الأصدقاء:** لا تقبل إضافات من حسابات مجهولة، فقد تكون "حسابات جمع بيانات" تستخدم صورك لتوليد التزييف العميق.
- **خصوصية الصور:** اجعل منشوراتك وصورك متاحة "للأصدقاء فقط" وليس للعامة، لتقليل المواد المتاحة لخوارزميات الذكاء الاصطناعي.

كيفية تأمين الصور الشخصية على السحاب (iCloud/Google Photos) لمنع المبتز من الوصول للمواد الخام التي قد يستخدمها في التزييف:

تأمين التخزين السحابي (Cloud Storage) أمر حيوي، لأن الوكالات الاستخباراتية أو المخترقين يعتبرونه "المنجم الذهبي" للمواد الخام (صورك وفيديوهاتك) التي تُستخدم لاحقاً في التزييف العميق أو الابتزاز.

إليك الخطوات التقنية لتأمين **ICloud** و **Google Photos** بأقصى درجة:

1-تأمين حساب آبل(iCloud):

آبل توفر ميزة ثورية تجعل حتى موظفي آبل أنفسهم غير قادرين على رؤية صورك:

- **تفعيل الحماية المتقدمة للبيانات:(Advanced Data Protection)**
  - ❖ اذهب إلى الإعدادات <اسمك < iCloud <الحماية المتقدمة للبيانات.
  - ❖ عند تفعيلها، يتم تشفير صورك ونسخك الاحتياطية بأسلوب "الطرفين End-to-End " (Encryption.هذا يعني أن مفتاح التشفير موجود على جهازك فقط، وليس لدى آبل.
- **مفاتيح الأمان الفيزيائية:** يمكنك إضافة YubiKey لحساب آبل، بحيث لا يمكن لأي شخص تسجيل الدخول للحساب من جهاز جديد إلا بوضع المفتاح يدوياً في الهاتف.

2- تأمين صور جوجل(Google Photos):

جوجل لا توفر تشفيراً كاملاً للطرفين مثل آبل (إلا في حالات محدودة)، لذا الاعتماد يكون على منع الوصول للحساب:

- **المجلد المقفل:(Locked Folder):**
  - ❖ انقل الصور الحساسة جداً إلى "المجلد المقفل" داخل تطبيق صور جوجل.
  - ❖ هذه الصور تُحذف من السحاب وتُخزن فقط على ذاكرة هاتفك وتُقفل ببصمتك، مما يمنع تسربها حتى لو تم اختراق حساب البريد الإلكتروني.
- **مراجعة الأجهزة المتصل:** اذهب إلى إعدادات حساب جوجل <**الأمان** <**إدارة جميع الأجهزة** .احذف أي جهاز قديم أو غير معروف فوراً.

3-إعدادات وقائية عامة للسحاب:

- **إيقاف الرفع التلقائي (Auto-Sync):** إذا كنت تلتقط صوراً حساسة، عطل ميزة المزامنة التلقائية. قم برفع الصور التي تريدها فقط يدوياً بعد التأكد من سلامتها.

- **تعطيل "مشاركة الموقع" في الصور:** الصور تحتوي على بيانات مخفية (EXIF) تحدد مكان التقاط الصورة بالضبط. قم بتعطيل ميزة "الموقع الجغرافي" في إعدادات الكاميرا لمنع السحاب من تخزين خريطة تحركاتك عبر صورك.
- **كلمة مرور مستقلة:** تأكد أن بريدك المرتبط بالسحاب له كلمة مرور فريدة لا تستخدمها في أي موقع آخر (مثل فيسبوك أو المنتديات) لضمان عدم تسريبها.

4- خيار "السحاب الشخصي" (للمحترفين):

إذا كنت لا تثق بالشركات الكبرى (جوجل وآبل)، يمكنك استخدام **السحاب المشفر** مثل:

- **Proton Drive:** يوفر تشفيراً كاملاً للطرفين ومقره في سويسرا (قوانين خصوصية صارمة).
- **Internxt:** سحاب يعتمد على تقنية "البلوكشين" وتجزئة الملفات، مما يجعل اختراقه شبه مستحيل.

نصيحة ذهبية: دائماً افترض أن أي شيء مرفوع على السحاب "قد" يُكشف يوماً ما. لذا، احتفظ بالبيانات الأكثر حساسية على **وحدة تخزين خارجية (External Drive)** مشفرة وغير متصلة بالإنترنت(Cold Storage).

كيفية تشفير وحدة تخزين خارجية (USB أو Hard Drive) لتكون خزنتك الرقمية الحصينة بعيداً عن الإنترنت:

تشفير وحدة تخزين خارجية (USB أو Hard Drive) يحولها إلى "خزنة رقمية" لا يمكن فتحها حتى لو سُرقت أو صودرت، وهي أفضل وسيلة لحفظ الصور والمستندات الحساسة بعيداً عن أعين وكالات الاستخبارات والمتسللين.

إليك أفضل الأدوات والطرق حسب نظام التشغيل الذي تستخدمه:

1- لمستخدمي ويندوز: أداة BitLocker:

هي أداة مدمجة في نسخ Windows Pro و Enterprise، وتتميز بالسرعة والموثوقية:

- **الطريقة:** اضغط بيمين الفأرة على وحدة التخزين (USB) واختر Turn on BitLocker.
- **الإعداد:** اختر كلمة مرور قوية جداً. سيعطيك النظام "مفتاح استرداد" (Recovery Key)؛ قم بطباعته ووضعه في مكان ورقي آمن.
- **الميزة:** بمجرد نزع الوحدة، تصبح البيانات مشفرة بالكامل ولا تفتح إلا بكلمة السر عند توصيلها مجدداً.

2. لمستخدمي ماك Disk Utility (macOS):

آبل توفر تشفيراً قوياً مدمجاً في النظام:

- **الطريقة:** افتح تطبيق Disk Utility، اختر الوحدة الخارجية، ثم اضغط Erase.
- **التشفير:** من قائمة "Format"، اختر APFS (Encrypted).
- **الميزة:** تشفير "عسكري" يتكامل بسلاسة مع بصمة الوجه أو الأصابع في أجهزة الماك.

3. الخيار الأقوى والمستقل VeraCrypt (لجميع الأنظمة):

هذا هو الخيار المفضل للمهتمين بالخصوصية القصوى (صحفيين، نشطاء، خبراء أمن)، لأنه برنامج مفتوح المصدر ولا تملكه أي شركة قد تتعاون مع الحكومات.

- **الميزة الكبرى (النفي المقنع – Plausible Deniability):** يتيح لك إنشاء "خزنة داخل خزنة". إذا أُجبرت على إعطاء كلمة المرور، يمكنك إعطاء كلمة مرور تفتح ملفات "عادية"، بينما تظل الملفات الحقيقية مخفية في جزء مشفر آخر لا يمكن إثبات وجوده أصلاً.

- **كيفية الاستخدام:** قم بتحميله من (veracrypt.fr)، اختر Create Volume، ثم اتبع الخطوات لتشفير القسم بالكامل.

4. وحدات التخزين ذات "لوحة المفاتيح" (Hardware Encrypted):

إذا كانت ميزانيتك تسمح، يمكنك شراء وحدات تخزين مثل **Apricorn Aegis** أو **Kingston IronKey**.

- **الميزة:** تحتوي هذه الوحدات على أزرار فيزيائية على جسمها. يجب إدخال الرمز يدوياً على الجهاز نفسه قبل توصيله بالكمبيوتر.
- **الأمان:** إذا حاول شخص إدخال الرمز بشكل خاطئ عدة مرات (مثلاً 10 مرات)، تقوم الوحدة بمسح وتدمير كافة البيانات بداخلها تلقائياً.

نصائح هامة للتخزين الفيزيائي:

- **لا تترك الوحدة متصلة:** لا تترك الـ USB متصلاً بالكمبيوتر طوال الوقت؛ صِلّه فقط عند الحاجة ثم افصله فيزيائياً.
- **النسخ المتعدد:** التشفير يحمي من "التلصص" ولكنه لا يحمي من "تلف الجهاز". احتفظ بنسخة مشفرة أخرى في مكان جغرافي مختلف.
- **تجنب الضياع:** تذكر أن ضياع كلمة المرور لوحدة مشفرة يعني فقدان البيانات للأبد؛ لا توجد وسيلة لاستعادتها.

كيفية التخلص الآمن من الأجهزة القديمة (إتلاف البيانات) بحيث لا يمكن لأي مختبر جنائي استعادتها:

عند التخلص من هاتف أو وحدة تخزين قديمة، لا يكفي مجرد "حذف" الملفات أو عمل "فورمات" عادي، لأن برامج الاستعادة الجنائية التي تستخدمها وكالات الاستخبارات يمكنها استرجاع البيانات بسهولة.

تاليا الطرق الاحترافية لضمان الإتلاف النهائي للبيانات:

1. للهواتف الذكية (iPhone & Android):

- التشفير أولاً: قبل القيام بأي خطوة، تأكد أن هاتفك مشفر (في الآيفون هو مشفر تلقائياً، وفي الأندرويد تأكد من الإعدادات). هذا يضمن أنه حتى لو استُرجعت البيانات، ستكون مجرد رموز غير مفهومة.
- إعادة ضبط المصنع (Factory Reset): قم بإجراء "إعادة ضبط المصنع" من داخل الإعدادات.
- طريقة "الملء والمسح" (اختياري للأمان الفائق): بعد الفورمات، قم بتعبئة ذاكرة الهاتف بملفات غير هامة (مثل فيديوهات عشوائية للطبيعة أو ملفات كبيرة لا قيمة لها) حتى تمتلئ الذاكرة تماماً، ثم قم بعمل فورمات مرة أخرى. هذا يضمن "الكتابة فوق" (Overwriting) البيانات القديمة الأصلية.

2. لوحدات التخزين (Hard Drive & USB):

- المسح الآمن (Secure Erase): استخدم برامج متخصصة مثل DBAN أو Eraser. هذه البرامج لا تحذف الملفات فقط، بل تكتب فوق كل "بت" (Bit) في القرص بيانات عشوائية عدة مرات (تصل إلى 7 أو 35 مرة) بناءً على معايير عسكرية (مثل معيار وزارة الدفاع الأمريكية DoD 5220.22-M).

- لأقراص الـ SSD: استخدم الأداة الرسمية من الشركة المصنعة (مثل Samsung Magician)، لأن أقراص SSD تعمل بطريقة مختلفة وتحتاج لأمر "Secure Erase" الخاص بها لضمان إفراغ الخلايا تماماً.

3. الإتلاف الفيزيائي (الحل الجذري):

إذا كانت البيانات بالغة الحساسية، فإن الإتلاف البرمجي قد لا يكون كافياً، والحل هو تدمير القطعة يدوياً:

- أقراص الـ HDD: يجب فتح القرص وخدش الأسطوانات المعدنية بآلة حادة أو كسرها.
- أقراص الـ SSD والـ USB: يجب تحديد "رقاقة الذاكرة" (Flash Chip) داخل الجهاز وكسرها أو طحنها.
- تحذير: لا تحاول حرق الأجهزة أو البطاريات لأنها تفرز غازات سامة وقد تنفجر.

4. لا تنسَ "نزع" القطع الخارجية: قبل بيع أو رمي الجهاز، تأكد من إزالة:

- شريحة الاتصال (SIM Card).
- بطاقة الذاكرة الخارجية (MicroSD).

هذه القطع غالباً ما تُنسى وهي تحتوي على قائمة الأسماء، الرسائل، وتاريخ المواقع الجغرافية.

تتبع شخص من صوته فقط؟ ولو استخدم جهاز او موبايل شخص اخر وفي مكان اخر او بلد اخر هل يمكن تتبعه من صوته:

يمكن ذلك تقنياً وبدقة عالية جداً. الوكالات الاستخباراتية المتطورة لم تعد تعتمد فقط على تتبع "الجهاز" (الرقم أو الـ IMEI)، بل انتقلت إلى تتبع "البصمة الحيوية" للشخص، وأهمها البصمة الصوتية (Voiceprint).

تاليا كيف تتم هذه العملية حتى لو غيرت الجهاز أو البلد:

1. البصمة الصوتية:

مثل بصمة الإصبع، لكل إنسان "بصمة صوتية" فريدة تتشكل من (سرعة الكلام، مخارج الحروف، ترددات الحنجرة، شكل التجويف الأنفي والفمي). الذكاء الاصطناعي يقوم بتحويل هذه الخصائص إلى نموذج رياضي رقمي يستحيل تزويره أو تغييره بسهولة.

2. التتبع عبر "الكلمات المفتاحية" (Keywords):

تمتلك الوكالات أنظمة مراقبة ضخمة (مثل نظام ECHELON) تقوم بمسح ملايين المكالمات والاتصالات عبر الأقمار الاصطناعية وكابلات الإنترنت البحرية.

- تعمل هذه الأنظمة بالذكاء الاصطناعي لرصد كلمات مفتاحية معينة أو بصمات صوتية محددة لأشخاص مطلوبين.
- بمجرد أن يتحدث الشخص المستهدف في "أي ميكروفون" متصل بالشبكة، يطلق النظام "تنبيهًا" (Alert) للمحللين.

3. هل يفيد تغيير الجهاز أو البلد؟

في حالة الاستهداف الاستخباراتي عالي المستوى، الإجابة هي **لا**، للأسباب الآتية:

- عزل الصوت (Speaker Identification): الأنظمة الحديثة قادرة على عزل صوت الشخص عن ضجيج الشارع أو جودة الميكروفون الضعيفة، ومطابقته بقاعدة البيانات في ثوانٍ.

- الشبكة العالمية: وكالات الاستخبارات (مثل العيون الخمس) تتشارك البيانات عالمياً. فإذا كان صوتك مسجلاً في قاعدة بيانات دولة ما، يمكن التعرف عليك بمجرد استخدامك لشبكة الاتصالات في دولة أخرى.
- تتبع الأنماط: حتى لو استخدمت هاتف شخص آخر، النظام يلاحظ أن هذا الهاتف بدأ يتحدث منه شخص يحمل "بصمة صوتية" معينة في وقت معين، ويبدأ بربط الموقع الجغرافي الجديد بالهوية الأصلية.

4. **كيف يمكن "التمويه" أو الحماية؟**

- استخدام تطبيقات مشفرة بالكامل: تطبيقات مثل Signal تشفر الصوت "من الطرفين"، مما يعني أن شركات الاتصالات أو أنظمة التنصت على الكابلات لا تسمع سوى "ضجيج مشفر" ولا يمكنها تحليل البصمة الصوتية.
- تغيير نبرة الصوت: تغيير الصوت يدوياً (التمثيل) قد يخدع البشر، لكنه نادراً ما يخدع الذكاء الاصطناعي الذي يحلل ترددات الحنجرة العميقة.
- أجهزة تشويش الصوت: توجد أجهزة احترافية تولد ضجيجاً أبيض (White Noise) حول المتحدث تجعل عملية "عزل الصوت" وتحليله برمجياً صعبة جداً.

الخلاصة: إذا كانت المكالمة تمر عبر "شبكة الاتصالات التقليدية" (GSM)، فإن الصوت هو هوية مكشوفة تماماً مهما تغير الجهاز أو المكان.

كيف يتم دمج تتبع الصوت مع تتبع الموقع لزيادة دقة المراقبة:

دمج تتبع الصوت مع الموقع الجغرافي هو ما يُعرف في عالم الاستخبارات بـ "الاستهداف المتعدد الوسائط"، وهو يجعل من المستحيل تقريبًا التخفي بمجرد إجراء اتصال واحد.

تعمل هذه المنظومة المتكاملة وفق الآتي:

1. **كيف يتم الدمج (Cross-Referencing)؟**

عندما يتحدث شخص مستهدف عبر هاتف "شخص آخر"، يقوم النظام بالآتي:

- تحديد الهوية بالصوت: يتعرف الذكاء الاصطناعي على بصمتك الصوتية فورًا.
- تحديد الموقع الفوري: بمجرد التعرف على الصوت، يقوم النظام بسحب بيانات برج الاتصال (Cell Tower) الذي يخرج منه الصوت، ليحدد دائرة جغرافية ضيقة لوجودك.
- تضييق النطاق: يُطلب من الهاتف (عبر أوامر خفية) إرسال إحداثيات الـ GPS أو فحص شبكات الـ Wi-Fi القريبة لتحديد مكانك بدقة أمتار قليلة.

2. **تطبيقات تحمي بصمتك الصوتية (وتمنع التتبع):**

للهروب من هذا الدمج، يجب استخدام تطبيقات تعتمد على "التشفير من الطرفين" وتخفي "البيانات الوصفية":

- Signal (الأفضل إطلاقاً):
  - ❖ تشفير الصوت: لا يمكن لأي جهة (حتى سيجنال نفسها) سماع الصوت أو تحليل بصمته.
  - ❖ إخفاء الـ IP (Relay Calls): كما ذكرنا سابقاً، يقوم سيجنال بتمرير مكالمتك عبر خوادمه، لذا لا يمكن لشركات الاتصالات أو المخترقين معرفة موقعك الجغرافي الحقيقي أثناء المكالمة.

- Threema:
  - ❖ لا يتطلب رقم هاتف للتسجيل، مما يقطع الرابط بين هويتك المادية وصوتك.
- Session:
  - ❖ يعمل بنظام "لامركزي" (نظام يشبه تور)، مما يجعل تتبع موقع المصدر مستحيلاً تقنياً.

3. مخاطر "الخلفية الصوتية" (Acoustic Fingerprinting):

الذكاء الاصطناعي لا يحلل صوتك فقط، بل يحلل الأصوات المحيطة بك لتحديد موقعك:

- إذا كنت تتحدث وفي الخلفية صوت قطار معين، أو نداء طائرة، أو حتى زقزقة عصافير نادرة، يمكن للنظام مطابقة هذه الأصوات بقواعد بيانات جغرافية لتخمين مدينتك أو مكانك بالضبط.

4. كيف تكسر حلقة التتبع (الصوت + الموقع)؟

1. استخدم تطبيقات الـ VoIP المشفرة: (مثل Signal) وتجنب المكالمات العادية تماماً.
2. فعل VPN دائماً: لتغيير موقعك الرقمي قبل إجراء المكالمة.
3. تحدث في مكان مغلق: لتقليل الضوضاء الخلفية التي قد تكشف موقعك الجغرافي.
4. استخدم ميزة "تغيير الصوت" (Voice Scramblers): في حالات التهديد القصوى، توجد أجهزة مادية تُركب على الميكروفون تقوم بتغيير ترددات الصوت قبل إرسالها للشبكة.

التشفير الكمي (Quantum Encryption) وهو الجيل القادم الذي تحاول الاستخبارات الوصول إليه لكسر كل هذه الحمايات:

يعتبر التشفير الكمي (Quantum Encryption) القفزة الكبرى القادمة في عالم الأمن الرقمي، وهو يمثل صراعاً محمومًا بين وكالات الاستخبارات التي تريد كسر كل الحمايات الحالية، وبين العلماء الذين يسعون لتأمين الاتصالات بشكل "يستحيل خرقه" بقوانين الفيزياء.

تاليا القصة ببساطة وكيف سيغير هذا التكنولوجيا مفهوم التجسس:

1. لماذا تخشى الاستخبارات "الحواسب الكمية"؟

التشفير الذي نستخدمه اليوم (مثل AES وRSA) يعتمد على مسائل رياضية معقدة جداً تستغرق الحواسيب الحالية آلاف السنين لحلها.

- المشكلة: الحواسيب الكمية (Quantum Computers) قادرة على حل هذه المسائل في ثوانٍ معدودة.
- النتيجة: بمجرد امتلاك دولة ما لحاسوب كمي قوي، ستصبح كل الرسائل المشفرة (حتى المخزنة من سنوات) مكشوفة تماماً أمامها. هذا ما يُعرف بـ "الهجوم الاسترجاعي" (احصد الآن، وفك التشفير لاحقاً).

2. الحل: توزيع المفتاح الكمي (QKD):

هذا هو "السحر" في التشفير الكمي. بدلاً من إرسال مفتاح التشفير عبر الإنترنت العادي، يتم إرساله عبر جسيمات الضوء (الفوتونات):

- قاعدة الفيزياء: في ميكانيكا الكم، "الملاحظة تغير الواقع". إذا حاول أي جاسوس أو جهاز استخباراتي اعتراض "الفوتون" لقياسه (التنصت عليه)، ستتغير حالة الفوتون فوراً.

- التنبيه الفوري: سيعرف المرسل والمستقبل فوراً أن هناك من حاول التجسس، ويتم تدمير المفتاح وتوليد مفتاح جديد تلقائياً. التجسس هنا يترك أثراً فيزيائياً لا يمكن إخفاؤه.

3. **السباق الاستخباراتي الحالي (الصين vs أمريكا):**

- الصين: تتصدر العالم حالياً؛ فقد أطلقت القمر الاصطناعي "ميسيوس" الذي أجرى أول اتصال فيديو مشفر كمياً وغير قابل للاختراق بين بكين وفيينا.
- أمريكا: تستثمر المليارات عبر وكالة "NSA" لتطوير ما يسمى بـ "التشفير ما بعد الكم" (Post-Quantum Cryptography)، وهو تشفير برمجي جديد لا تستطيع حتى الحواسيب الكمية كسر ميزاته الرياضية.

4. **كيف سيؤثر ذلك عليك مستقبلاً؟**

لن تحتاج لشراء حاسوب كمي، ولكن الشركات التي تقدم لك الخدمات (مثل Signal أو Apple) ستبدأ تدريجياً في تحديث خوارزمياتها لتكون "مقاومة للكم".

- ابل (Apple): قامت بالفعل بإطلاق بروتوكول PQ3 لتطبيق iMessage، وهو نظام تشفير مصمم لمقاومة الهجمات المستقبلية من الحواسيب الكمية.

5. هل يعني هذا نهاية التجسس؟

لا، بل سيعود التجسس إلى "العنصر البشري". عندما يصبح كسر التشفير مستحيلاً فيزيائياً، ستلجأ الاستخبارات إلى:

- زرع عملاء ماديين.
- سرقة الأجهزة وهي مفتوحة.
- ابتزاز الأشخاص للحصول على كلمات المرور.

الخلاصة: نحن ننتقل من عصر "الرياضيات الصعبة" إلى عصر "الفيزياء المستحيلة".

استخدام الكتابة بدل المكالمات الصوتية:

إجابة هذا الموضوع تعتمد على نوع التطبيق الذي تستخدمه، ولكن من الناحية التقنية والاستخباراتية، يمكن القول إن الكتابة عبر تطبيقات مشفرة آمن بكثير من المكالمات الصوتية التقليدية، وإليك الأسباب:

1. **سهولة الاعتراض (Interception):**

- المكالمات الصوتية: إذا كانت مكالمة عادية (GSM)، فهي تمر عبر أبراج الاتصالات وتكون مكشوفة تماماً لأنظمة "البصمة الصوتية" والكلمات المفتاحية التي ناقشناها.
- الكتابة (المشفرة): في تطبيقات مثل Signal، تتحول الرسالة إلى كود معقد قبل خروجها من جهازك، ولا يمكن فك شفرتها إلا بجهاز الطرف الآخر. حتى لو تم اعتراضها في منتصف الطريق، ستبدو كرموز عشوائية.

2. **"الأثر الرقمي" الدائم (Digital Footprint)**

هنا تتفوق المكالمات في نقطة واحدة:

- المكالمات: بمجرد انتهاء المكالمة، لا يوجد "سجل" لمحتواها (ما لم تكن مُسجلة).
- الكتابة: الرسائل تبقى مخزنة على الجهازين. إذا صودر هاتف الطرف الآخر، ستكون محادثاتك مكشوفة.

الحل: استخدم خاصية "الرسائل المختفية" (Disappearing Messages) لتجعل الكتابة تتفوق على الصوت في الأمان.

3. البصمة الحيوية (Biometrics):

- الصوت: كما ذكرنا، صوتك هو "بصمة" لا تتغير وتكشف هويتك وموقعك عبر تحليل الترددات.
- الكتابة: لا تحمل بصمة حيوية (إلا إذا تم تحليل أسلوبك في الكتابة "Stylometry"، وهو أمر أصعب بكثير ويحتاج لنصوص طويلة جداً للقيام به).

4. بيانات الموقع (Metadata):

- في المكالمات العادية، تضطر شركات الاتصالات لتسجيل موقع البرج الذي استخدمته طوال مدة المكالمة.
- في الكتابة عبر تطبيقات محمية بـ **VPN**، يكون من الصعب جداً ربط الرسالة بموقعك الجغرافي الدقيق.

الخلاصة: أيهما تختار؟

- **الأكثر أماناً:** الكتابة عبر تطبيق **Signal** مع تفعيل **الرسائل المختفية** (مثلاً بعد 30 ثانية أو دقيقة). هذا يجمع بين ميزة "التشفير القوي" وميزة "عدم وجود سجل" بعد المحادثة.
- **الأكثر خطورة:** المكالمات الصوتية التقليدية (عبر شريحة الهاتف)؛ فهي "كتاب مفتوح" لأي جهة استخباراتية.
- **نصيحة للمحترفين:** إذا اضطررت للمكالمة، استخدم **مكالمات البيانات (VoIP)** داخل تطبيقات مشفرة مثل Signal أو WhatsApp، مع تفعيل خاصية "إخفاء عنوان IP" في الإعدادات، فهي آمنة بمراحل من المكالمة العادية.

تفعيل ميزة "تدمير الرسائل ذاتياً" في مختلف التطبيقات لضمان عدم بقاء أي أثر للكتابة:

تفعيل ميزة "التدمير الذاتي" أو "الرسائل المختفية" هي الخطوة التي تحول الكتابة من "سجل دائم" إلى "محادثة عابرة" تشبه الكلام الشفهي الذي يختفي بمجرد النطق به.

إليك كيفية تفعيلها في التطبيقات الأكثر أماناً:

1. تطبيق سيجنال (Signal) – الأمان الأقصى:

سيجنال يتيح لك ضبط مؤقت شامل لكل المحادثات الجديدة تلقائياً:

- الطريقة: اذهب إلى الإعدادات > الخصوصية > الرسائل المختفية > المؤقت الافتراضي للمحادثات الجديدة.
- الخيارات: يمكنك الاختيار من 30 ثانية إلى 4 أسابيع.
- الميزة: بمجرد رؤية الطرف الآخر للرسالة، يبدأ العد التنازلي وتُحذف الرسالة من الجهازين ومن "سيرفرات" الشركة تماماً.

2. تطبيق واتساب (WhatsApp):

واتساب أضاف هذه الميزة مؤخراً وهي فعالة جداً لتقليل الأثر الرقمي:

- لكل المحادثات: الإعدادات > الخصوصية > مؤقت الرسائل التلقائي.
- لمحادثة محددة: اضغط على اسم الشخص داخل المحادثة > الرسائل ذاتية الاختفاء.

- ميزة "العرض لمرة واحدة" (View Once): عند إرسال صورة أو فيديو، اضغط على رقم (1) الصغير بجانب زر الإرسال. ستختفي الصورة فور إغلاقها ولا يمكن حفظها في معرض الصور.

3. تطبيق تليجرام (Telegram) – "المحادثات السرية" فقط:

تنبيه هام: الرسائل العادية في تليجرام ليست مشفرة من الطرفين افتراضياً. لتفعيل التدمير الذاتي، يجب استخدام:

- المحادثة السرية (Secret Chat): اضغط على اسم الشخص > "المزيد" (أو الثلاث نقاط) > بدء محادثة سرية.
- ضبط المؤقت: داخل المحادثة السرية، اضغط على أيقونة الساعة واختر الوقت (من ثانية واحدة إلى أسبوع). أي شيء يُكتب هنا سيُحذف ولا يمكن للطرف الآخر أخذ لقطة شاشة (Screenshot) دون تنبيهك.

4. تطبيق إنستجرام (Instagram) – وضع الفانيش:

- Vanish Mode: داخل أي محادثة، قم بسحب الشاشة من الأسفل إلى الأعلى. ستتحول الشاشة للون الأسود، وبمجرد خروجك من المحادثة، ستُحذف جميع الرسائل التي قُرئت تلقائياً.

نصائح "بروتوكول الأمان" عند استخدام الرسائل المختفية:

1. اختر وقتاً قصيراً: إذا كنت تناقش أموراً حساسة جداً، اجعل المؤقت أقل من 5 دقائق.
2. تذكر "لقطات الشاشة": رغم أن التطبيقات تحاول منعها أو التنبيه عنها، إلا أن الطرف الآخر يمكنه دائماً تصوير شاشة هاتفه بكاميرا هاتف آخر. لذا، الثقة في الطرف الآخر تظل هي الركيزة الأساسية.
3. تجنب النسخ الاحتياطي: تأكد من تعطيل النسخ الاحتياطي (Cloud Backup) للمحادثات، لأن الرسائل قد تُحفظ في السحاب قبل أن يتم تدميرها ذاتياً في الهاتف.

إخفاء أيقونة التطبيقات الحساسة (مثل Signal) من شاشة هاتفك تماماً بحيث لا يراها أي شخص يمسك بهاتفك؟، هذا هو المستوى الأخير من التمويه المادي.

إخفاء أيقونة التطبيقات هو إجراء أمني فيزيائي يمنع أي شخص يمسك بهاتفك (سواء في نقطة تفتيش أو في حالة الفقدان) من معرفة البرامج التي تستخدمها للتواصل.

إليك كيفية القيام بذلك في الأنظمة المختلفة:

1. هواتف أندرويد (الخيار الأقوى):

توفر معظم هواتف أندرويد ميزات مدمجة لإخفاء التطبيقات تماماً:

- **هواتف سامسونج:**
  - ❖ اضغط مطولاً على الشاشة الرئيسية > إعدادات الشاشة الرئيسية > إخفاء التطبيقات.
  - ❖ اختر التطبيقات (مثل Signal)، ولن تظهر في قائمة التطبيقات أو الشاشة الرئيسية. للوصول إليها، يجب البحث عنها بالاسم في شريط البحث.
- استخدام المجلد الآمن (Secure Folder): يمكنك نقل التطبيق لداخل "المجلد الآمن" ثم إخفاء أيقونة المجلد نفسه من قائمة الإشعارات.

- تغيير شكل الأيقونة (App Disguise): تتيح بعض الواجهات (مثل تطبيقات Launcher) تغيير شكل أيقونة "Signal" لتظهر كأنها "آلة حاسبة" أو "لعبة عادية" وتغيير اسمها أيضاً.

2. هواتف آيفون (iOS):

آبل لا تسمح بإخفاء التطبيق بكلمة سر مستقلة، ولكن يمكنك تمويه وجوده:

- الإزالة من الشاشة الرئيسية: اضغط مطولاً على التطبيق > إزالة التطبيق > الإزالة من الشاشة الرئيسية. سيبقى التطبيق موجوداً فقط في "مكتبة التطبيقات" (App Library) في آخر صفحة يميناً.
- إخفاء من البحث والاقتراحات: اذهب إلى الإعدادات > Siri والبحث > اختر التطبيق (Signal) > قم بإيقاف جميع الخيارات (مثل "إظهار في البحث"). بهذا، لن يظهر التطبيق حتى لو قام شخص بالبحث عنه داخل الهاتف.
- استخدام المجلدات: ضع التطبيق في الصفحة الثانية أو الثالثة داخل مجلد يحتوي على تطبيقات عادية (مثل تطبيقات الإنتاجية أو الصحة) للتمويه.

3. التطبيقات ذات "الواجهة الوهمية" (للمحترفين):

توجد تطبيقات تُسمى "**App Hiders**" على متجر Google Play، تقوم بإنشاء مساحة موازية مخفية:

- تظهر هذه التطبيقات على الشاشة كأنها "آلة حاسبة" بسيطة تعمل فعلياً.
- عند إدخال رمز سري معين (مثلاً 1234=) داخل الآلة الحاسبة، تفتح واجهة سرية تحتوي على تطبيقاتك المخفية.

4. نصيحة "إشعارات التمويه":

لا يهم إذا أخفيت الأيقونة بينما تظهر رسالة "Signal: كيف حالك؟" على شاشة القفل!

- **الإجراء:** اذهب لإعدادات الإشعارات داخل التطبيق نفسه واجعلها "**لا تظهر المحتوى**" (Show no content) أو اجعلها تظهر "رسالة جديدة" فقط دون اسم المرسل أو النص.

نصيحة ذهبية: في حالات الخطر القصوى، يُفضل عدم بقاء التطبيق على الهاتف أصلاً. تطبيقات مثل **Session** تتيح لك حذف التطبيق وتثبيته لاحقاً واستعادة محادثاتك عبر "مفتاح الاستعادة" دون الحاجة لربطها برقم هاتف أو بريد.

مدى الأمان في تطبيق سيجنال:

تطبيق سيجنال (Signal) آمن إلى أبعد مدى تتيحه التكنولوجيا الحالية، ولكن بشرط فهم "حدود" هذا الأمان. سيجنال ليس "سحراً"، بل هو بروتوكول تشفير قوي جداً يعالج نقاط الضعف التي تتركها التطبيقات الأخرى مكشوفة. إليك تحليل دقيق لمدى أمانه:

1. لماذا يعتبره الخبراء (مثل إدوارد سنودن) الأفضل؟

- تشفير المحتوى (End-to-End Encryption): سيجنال يستخدم بروتوكولًا مفتوح المصدر يُعد "المعيار الذهبي" عالمياً. الرسائل تُشفر على جهازك ولا تُفك شفرتها إلا على جهاز المستلم. لا تستطيع الشركة، ولا مزود الإنترنت، ولا أي جهة استخباراتية اعتراض المحتوى وقراءته أثناء مروره في الشبكة.

- الحد الأدنى من البيانات الوصفية (Metadata): هذا هو الفرق الجوهري عن "واتساب". واتساب يعرف مع من تتحدث، ومتى، ومن أين. أما سيجنال، فهو لا يخزن عنك سوى تاريخ إنشاء الحساب وآخر تاريخ للاتصال بالخادم فقط. إذا طالبت جهة أمنية سيجنال ببياناتك، فلن يجدوا شيئاً يقدمونه.
- مفتوح المصدر (Open Source): الكود البرمجي للتطبيق متاح للجميع لمراجعته. هذا يعني أنه لا توجد "أبواب خلفية" (Backdoors) مخفية للاستخبارات؛ لأن المبرمجين حول العالم سيكتشفونها فوراً.

2. نقاط القوة "الاستخباراتية" في سيجنال:

- إخفاء الـ IP (Relay Calls): كما ذكرنا، يمنع تتبع موقعك الجغرافي أثناء المكالمات.
- أمن الشاشة: يمنع ظهور محتوى الرسائل في قائمة التطبيقات المفتوحة، ويمكن ضبطه لمنع أخذ لقطات شاشة.
- قفل التسجيل: يمنع سرقة حسابك حتى لو تم اختراق شريحة الهاتف (SIM Swapping).

3. "إلى أي مدى"؟ (أين تكمن الخطورة؟):

الأمان في سيجنال ينتهي عند **أطراف الجهازين**، أي أن التطبيق آمن طالما أن:

1. هاتفك في يدك: إذا تم اختراق نظام تشغيل هاتفك ببرمجية تجسس (مثل بيغاسوس)، فإن المخترق سيشاهد الرسائل "من داخل الجهاز" بعد فك تشفيرها، وهنا لا ينفع تشفير التطبيق.
2. ثقتك في الطرف الآخر: التشفير يحمي الرسالة من "المتنصت"، لكنه لا يحميها من "المستلم" إذا قرر تصوير الشاشة أو تسريب المحادثة.
3. تأمين النسخ الاحتياطي: سيجنال لا يقوم بعمل نسخ احتياطي سحابي (Cloud Backup) افتراضياً، وهذا قمة الأمان. إذا قمت بعمل نسخة احتياطية يدوية غير مشفرة، فأنت تكسر أمان التطبيق بنفسك.

الخلاصة: سيجنال هو أقوى أداة مراسلة مدنية متاحة اليوم. هو يحميك تماماً من "التنصت الشامل" و"جمع البيانات" و"تتبع الشبكة". ولكنه لا يحميك من "اختراق نظام الهاتف" نفسه أو "الخيانة" من الطرف الآخر.

القائمة النهائية والمختصرة للحماية (The Ultimate Security Checklist):

يمكن نسخها والاحتفاظ بها في "الملاحظات المقفلة" بالهاتف لتكون مرجع دائم للأمان الرقمي:

1. تأمين الجهاز (المستوى الفيزيائي والنظام):

- إعادة التشغيل اليومي: لقطع اتصال أي برمجية تجسس نشطة في الذاكرة.
- تحديثات النظام: تفعيل التحديث التلقائي لسد ثغرات "يوم الصفر" (Zero-day).
- وضع الإغلاق (Lockdown Mode): تفعيله في الآيفون عند التواجد في أماكن عالية الخطورة.
- قفل شريحة الـ SIM: وضع رمز PIN للشريحة لمنع سرقة الرقم (SIM Swapping).

2. تأمين المراسلات (بروتوكول سيجنال):

- الرسائل المختفية: ضبط المؤقت الافتراضي لجميع المحادثات (مثلاً 5 دقائق أو يوم واحد).
- إخفاء عنوان IP: تفعيل خيار (Relay Calls) في إعدادات خصوصية المكالمات.
- تأمين الشاشة: تفعيل قفل التطبيق ببصمة الوجه أو رمز مستقل عن رمز الهاتف.

3. تأمين الحسابات (إدارة الهوية):

- مدير كلمات المرور (Bitwarden): استخدام كلمات سر فريدة ومعقدة لكل حساب.
- المصادقة الثنائية (FA2): استخدام تطبيقات المصادقة (Google Authenticator) والابتعاد عن الـ SMS.
- فحص التسريبات: مراجعة موقع (Have I Been Pwned) دورياً للتأكد من سلامة بريدك الإلكتروني.

4. التمويه والحماية المادية:

- إخفاء الأيقونات: إزالة تطبيقات المراسلة الحساسة من الشاشة الرئيسية وتفعيل "إخفاء المحتوى" في الإشعارات.
- حقيبة فارادي: وضع الهاتف داخلها أثناء الاجتماعات الهامة أو عند الرغبة في العزل التام عن التتبع الجغرافي.
- التشفير السحابي: تفعيل (Advanced Data Protection) في iCloud أو استخدام "المجلد المقفل" في Google Photos.

5. القاعدة الذهبية (الوعي الفطري):

- قاعدة الـ 30 ثانية: قبل الضغط على أي رابط أو تحميل أي ملف، توقف وفكر: "لماذا وصلني هذا الآن؟".
- تجنب شبكات الواي فاي العامة: استخدم دائماً الـ VPN أو بيانات الهاتف الخاصة بك.

نسخة احتياطية تنقذك إذا فقد هاتفك او نسيت كلمة المرور الرئيسة:

نسخة احتياطية ورقية (Emergency Recovery Kit): إجراء ينقذك إذا فقدت هاتفك، أو نُسيت كلمة المرور الرئيسية، أو تعطلت وسيلة المصادقة الثنائية. في عالم التشفير القوي، "الورقة" هي الوسيلة الوحيدة التي لا يمكن اختراقها عن بُعد. إليك كيفية إعدادها وتأمينها:

1-ماذا تضع في هذه الورقة؟

يجب أن تحتوي الورقة على "مفاتيح العودة" التي لا يمكن استردادها عبر البريد الإلكتروني:

- كلمة المرور الرئيسية: لمدير كلمات المرور مثل Bitwarden.
- رموز الاستعادة (Recovery Codes): وهي الرموز التي تعطيها لك شركات مثل Google, Apple, Microsoft عند تفعيل المصادقة الثنائية (FA2)؛ وتُستخدم لمرة واحدة إذا فقدت هاتفك.
- مفتاح استعادة سيجنال (Signal Recovery Code): الرمز المكون من 30 رقماً والذي يسمح لك باستعادة حسابك ومجموعاتك.
- مفاتيح تشفير الأقراص: مثل مفتاح استرداد (BitLocker) أو (FileVault) الخاص بجهاز الكمبيوتر.

2- كيف تكتبها وتؤمنها؟

- الكتابة اليدوية: يفضل كتابتها بخط اليد بدلاً من طباعتها، لمنع بقاء أي أثر رقمي لها في ذاكرة الطابعة أو الحاسوب.
- استخدام الرموز (التمويه): لا تكتب "كلمة سر سيجنال: 12345". بدلاً من ذلك، اكتب "رمز S: [كلمتك]"، ليفهمها أنت فقط في حال وقعت الورقة في يد شخص آخر.

- **التغليف (Lamination):** قم بتغليف الورقة بالبلاستيك لحمايتها من الرطوبة أو التلف مع مرور الزمن.

3- أين تخزنها؟ (التخزين الفيزيائي):

- الخزنة المنزلية: إذا كانت لديك خزنة حديدية مضادة للحريق.
- صندوق الأمانات: في البنك إذا كنت تفضل أقصى درجات الأمان المادي.
- مكان "غير متوقع": داخل كتاب قديم في مكتبتك، أو خلف لوحة معلقة، أو في مخبأ سري تعرفه أنت فقط.
- التوزيع الجغرافي: يفضل عمل نسختين؛ واحدة في منزلك والأخرى في مكان آمن آخر (مثل منزل العائلة) لضمان الوصول إليها في حال وقوع كارثة طبيعية أو حريق.

4-القاعدة الذهبية: "لا تصوّرها":

أكبر خطأ يقع فيه المستخدمون هو أخذ لقطة شاشة (Screenshot) لهذه الأكواد وحفظها في "الاستوديو". هذا يلغي كل ما ذكرناه؛ لأن أي اختراق للهاتف سيعطي المهاجم "مفاتيح المملكة" بالكامل.

المحور الثاني: حقيبة/ صندوق فارادي حماية بين يديك

ما هي حقيبة/ صندوق فراداي(Faraday Bag / Box) ؟

حقيبة أو صندوق فراداي هو غلاف مصنوع من مواد معدنية خاصة تمنع مرور الإشارات الإلكترونية من وإلى الجهاز بداخله. يعني ببساطة:

- عندما تضع هاتفك أو جهازك داخله فإنه يختفي تمامًا عن الشبكات (كأنه غير موجود).
- الفكرة تعتمد على مبدأ علمي اسمه "قفص فاراداي(Faraday Cage) "، حيث يتم امتصاص وإعادة توزيع الموجات الكهرومغناطيسية ومنعها من الدخول أو الخروج

ماذا تفعل بالضبط حقيبة/ صندوق فرادي؟

عند وضع جهاز داخلها:

- لا يوجد اتصال شبكة (4/G – 5/G).
- لا Wi-Fi.
- لا GPS (لا تتبع مواقع).
- لا Bluetooth.
- لا NFC أوRFID

بمعنى آخر: الجهاز معزول بالكامل عن العالم الخارجي.

استخداماتها الشائعة

1- الخصوصية والأمان:

- منع التجسس أو التتبع
- إخفاء موقع الهاتف

2- حماية مفاتيح السيارات:

- تمنع سرقة السيارات الحديثة(relay attack).
- لأنها تمنع إشارات المفتاح الذكي.

3-الأمن الرقمي / التحقيقات

تستخدمها الشرطة لحفظ الأدلة الرقمية.

4- الحماية من النبضات الكهرومغناطيسية(EMP):

بعض الأنواع تحمي الأجهزة من الكوارث الكهربائية.

أنواعها

1- حقيبة صغيرة(Faraday Pouch):

- للهاتف أو مفاتيح السيارة.
- رخيصة وخفيفة.

2- صندوق فاراداي(Faraday Box)

- أكبر، توضع فيه عدة أجهزة.
- أقوى عادة.

3- حقائب كبيرة:

للابتوب أو معدات كاملة.

أمثلة حقيقية:

- أفضل خيار بسيط للهاتف: Faraday Bag for Smart Phones
- خيار أقوى وأكثر احترافية Signal Killer Faraday Bag Large: حقيبة كبيرة بقدرة عالية لعزل الإشارات وحماية الأجهزة.
- صندوق فاراداي متطور Mission Darkness BlockBox Touch: صندوق احترافي يعزل الأجهزة تمامًا ويستخدم في الأمن والتحقيقات

ملاحظات مهمة:

- الجودة تختلف كثيرًا (بعض الرخيص لا يعمل جيدًا).
- يجب إغلاق الحقيبة بالكامل حتى تعمل.
- مع الوقت قد تضعف الطبقة المعدنية.

خلاصة: حقيبة فراداي عبارة عن درع رقمي يعزل جهازك عن أي اتصال أو تتبع.

أفضل الخيارات بكل الفئات (للخصوصية، لحماية السيارة، للسفر):

ترشيحات حقيقية مرتبة حسب الاستخدام: (هاتف – مفاتيح – حماية قوية – صناديق احترافية).

أولًا: أفضل حقيبة صغيرة للهاتف (Best overall):   Faraday Bag for Smart Phones

- مناسبة للاستخدام اليومي.
- تمنع: اتصالGPS – WiFi – Bluetooth.
- خفيفة وسهلة الحمل.

هذا النوع هو الأكثر شيوعًا لأنّه عملي وسريع.

ثانيًا: أفضل خيار لحماية مفاتيح السيارة: Leechio Faraday Bags (2 PCS)

حقيبتان صغيرتان لحماية مفاتيح السيارات من السرقة عبر الإشارة، حيث:

- تحمي من هجمات(relay سرقة السيارة بالإشارة).
- صغيرة جدًا (توضع في الجيب).
- حل اقتصادي.

كثير من سرقات السيارات الحديثة تعتمد على التقاط إشارة المفتاح، وهذه الحقيبة تمنع ذلك تمامًا.

ثالثًا: أفضل حقيبة قوية / احترافية: Mission Darkness TitanRF Faraday Sack

حقيبة احترافية بعزل قوي تستخدم للأمن الاستخباراتي الرقمي والمعدات، تمتاز :

- مستوى عزل عالي (عسكري تقريبًا).
- تستخدمها جهات أمنية.
- مناسبة لأجهزة متعددة.

بعض الشركات تصممها لتمنع إشارات من 200 MHz إلى 40 GHz مثل 4 G/5G و GPS

رابعًا: صندوق فاراداي (الأقوى): Mission Darkness BlockBox Touch

صندوق احترافي يعزل الأجهزة بالكامل ويستخدم في التحقيقات الرقمية، ويمتاز :

- عزل كامل 100% تقريبًا.
- يستخدم في الأمن والشرطة.
- يمكن وضع عدة أجهزة

هذا أقرب لـ "غرفة عزل صغيرة" وليس مجرد حقيبة.

نصائح مرتبطة بالهدف من الاستخدام:

- إذا كان الهدف الخصوصية اليومية: استخدم حقيبة هاتف.
- إذا كان الهدف حماية السيارة: استخدم حقيبة مفاتيح.
- إذا كان الهدف أمان قوي أو عمل تقني: استخدم حقيبة احترافية.
- إذا كان الهدف عزل كامل (100%): استخدم صندوق فاراداي.

تنبيهات مهمة: حتى أفضل الحقائب:

- قد تحتاج إغلاق محكم.
- بعض الأنواع الرخيصة لا تعزل بالكامل.
- أحيانًا تحتاج طبقتين لعزل أقوى (حسب تجارب المستخدمين).

كيف تختار حماية ذات مستوى عالي جدا:

تمنع من: التجسس + التتبع + الاختراق.

فسأعطيك أفضل الخيارات "المستوى العالي جدًا" (وليس العادي).

كيف تختار (مهم جدًا):

لتحقيق حماية حقيقية، ركّز على:

- عدد طبقات العزل (2–3 طبقات أو أكثر)
- قوة التوهين (100 db أو أعلى).

- إغلاق محكم 100% (Velcro + مغناطيس أو zip)
- اختبار عسكري(MIL-STD)

لأن الحقائب القوية فقط هي التي تمنع GPS + 5G + WiFi بالكامل.

افضل حماية للهواتف :Best Overall Mission Darkness TitanRF Faraday Sack

- عزل قوي جدًا (يستخدمه الأمن والشرطة).
- يمنع: GPS + 5G + Bluetooth + Wi-Fi.
- مناسب إذا تخاف من تتبع حقيقي.

هذا أقوى خيار "حقيبة" بدون الدخول في صناديق.

خيار احترافي تكتيكي (للعمل الأمني): حقيبة Mission Darkness MOLLE Faraday Pouch

حقيبة تكتيكية عسكرية تثبت على الحقيبة أو الحزام لعزل الأجهزة أثناء الحركة:

- تصميم عسكري(MOLLE).
- عملية أثناء التنقل.
- مستوى العزل عالي.

ممتاز لك إذا كنت تتحرك كثيرا وتريد حماية دائمة.

خيار شامل (عدة أجهزة + لابتوب): Faraday Laptop Bag Signal Blocking

حقيبة كبيرة تعزل لابتوب وأجهزة متعددة من التتبع والاختراق، هي:

- تحمي: هاتف + لابتوب + أجهزة.
- مناسبة للسفر أو العمل.
- عزل قوي متعدد الطبقات.

أقوى شيء في السوق (صندوق احترافي): صندوق Mission Darkness BlockBox Touch

صندوق احترافي يعزل الأجهزة 100% ويستخدم في التحقيقات الرقمية:

- عزل شبه كامل 100%.
- يستخدم في الأمن والطب الشرعي الرقمي.
- يمنع أي تسريب إشارات.

هذا أقوى من أي حقيبة، مستواه في مستوى أل "مختبر / استخبارات."

الخلاصة: الاختيار المثالي وفق هدفك:

- ♣ لحماية يومية قوية جدًا: TitanRF هو الأفضل
- ♣ لأقصى حماية ممكنة ضد التجسس الحقيقي: BlockBox Touch بدون نقاش.
- ♣ لحل شامل لكل أجهزتك: حقيبة اللابتوب.

تحذير مهم جدًا

- الهاتف داخل حقيبة فاراداي ويكون مخفي تمامًا عن الشبكة.
- لكن:
  - عند إخراجه يعود التتبع فورًا.
  - لا يحمي من اختراق داخل الجهاز نفسه (برمجيات).

يعني هو يحمي من:

- التتبع.
- والمراقبة عبر الشبكة.

لكن لا يغني عن:

- حذف التطبيقات المشبوهة.
- وإيقاف الأذونات.

لأفضل حماية حقيقية:

استخدم حقيبة قوية + عادات أمان رقمية، وليس الاعتماد على الحقيبة فقط.

بناء خطة حماية حقيقية قوية جدًا (مستوى متقدم) ضد:

التتبع – التجسس – الاختراق – المراقبة. مقسمة إلى طبقات وفق الآتي:

الطبقة الأولى: العزل الفيزيائي(Faraday):

الهدف: إخفاء جهازك بالكامل عند الحاجة، استخدم:

- حقيبة قوية مثل Mission Darkness TitanRF Faraday Sack
- أو صندوق مثل Mission Darkness BlockBox Touch

متى تستخدمها؟

- عند الاجتماعات الحساسة.
- أثناء السفر.
- عند عدم الحاجة للهاتف.

هذا يمنع:

- GPS.
- الأبراج.
- WiFi.
- أي تتبع مباشر.

الطبقة الثانية: تأمين الهاتف نفسه، أهم الإعدادات (ضرورية جدًا): إذا كنت تستخدم Android:

إيقاف:

- Location History
- Bluetooth scanning
- WiFi scanning
- إزالة أي تطبيق لا تعرفه

إذا كنت تستخدم iOS:

- حدد Privacy من Settings
- أغلق Location لمعظم التطبيقات.
- إيقاف:
  - Significant Locations
  - Tracking (App Tracking Transparency)

أهم خطوة يجب عدم تجاهلها: استخدم تطبيقات آمنة مثل:

- Signal (أفضل للمراسلة المشفرة).
- Proton VPN (إخفاء IP).

تجنب:

- التطبيقات المعدلة.
- الروابط المشبوهة.

الطبقة الثالثة: إخفاء الهوية على الإنترنت:

الهدف: عدم تتبعك أثناء التصفح

استخدم:

- متصفح Brave Browser.
- أو شبكة Tor.

يمنع:

- التتبع الإعلاني.
- بصمة الجهاز.

الطبقة الرابعة: التحكم في الشبكة: القواعد الذهبية:

- لا تستخدم WiFi مفتوح.

أوقف:

- Blutooth دائما.
- AirDrop في iPhone.

لأن هذه منافذ تجسس شائعة

الطبقة الخامسة: السلوك (الأهم فعليًا): حتى أقوى الأدوات لا تنفع بدون هذا:

إياك أن تفعل الآتي:

- إعطاء رقمك لأي جهة.
- الضغط على روابط مجهولة.
- استخدام ذات الحساب بكل مكان.

إذن، عليك أن:

- تستخدم رقم منفصل (SIM ثاني).
- قسم حياتك الرقمية بين: شخصي وعملي.

المستوى المتقدم من الحماية (إذا كنت قلق جدًا):

- استخدم هاتف منفصل "نظيف".
- لا تربطه بحساباتك الشخصية.
- استخدمه فقط عند الحاجة.

هذا يسمى: الأمن التشغيلي (Operational Security (OpSec

أهم نصيحة: أكبر خطر ليس التكنولوجيا… بل سلوك المستخدم

المحور الثالث: كيف تكتشف الاختراق، وكيف تبني هاتف "شبه غير قابل للتتبع"

أولًا: كيف تعرف أن جهازك مُخترق؟

علامات قوية (إذا رأيت أكثر من واحدة مما يلي فهذا يعني خطر حقيقي)

1-استهلاك بطارية غير طبيعي:

- الهاتف يسخن بدون سبب.
- البطارية تنفد بسرعة حتى بدون استخدام.

قد يعني وجود برنامج يعمل في الخلفية (Spyware)

2– نشاط شبكة غريب:

- استهلاك إنترنت عالي بدون سبب.
- بيانات تُرسل في الخلفية.

برامج التجسس ترسل بياناتك للخوادم.

3- سلوك غير طبيعي للهاتف:

- يفتح أو يغلق لوحده.
- تطبيقات تظهر فجأة.
- إعادة تشغيل عشوائية.

4- إشارات تجسس مباشرة:

- الميكروفون يعمل بدون سبب.
- الكاميرا تشتغل أو تضيء.

أدوات فحص مهمة:

على :Android

تطبيق:

- Malwarebytes
- Hypatia (Android security app)

على :iOS

استخدم:

- iMazing (لفحص النسخ الاحتياطي).

اختبار بسيط بنفسك:

1. فعل وضع الطيران:
2. راقب البطارية.

إذا استمر الاستهلاك العالي: المشكلة داخل الجهاز.

إذا توقف: غالبًا نشاط شبكة (تجسس)

إذا تأكدت من الاختراق، الحل الجذري (بدون نقاش):

1- فورًا:

- افصل الإنترنت
- أخرج الشريحة (SIM)

2-ثم:

- إعادة ضبط المصنع (Factory Reset)

3- الأفضل:

- لا تسترجع النسخة الاحتياطية.

لأن التجسس قد يعود مع النسخة

ثانيًا: كيف تصنع هاتف شبه غير قابل للتتبع

الهدف: تقليل التتبع إلى أدنى مستوى ممكن

المستوى الاحترافي الحقيقي: استخدم نظام بديل:

- GrapheneOS (الأقوى عالميا).
- أو CalyxOS
- بدون خدمات جوجل.
- تحكم كامل في الخصوصية.
- حماية عالية من الاختراق.

إذا لم تستطع تغيير النظام، قم بهذه الإعدادات:

إيقاف:

- Location دائمًا
- Bluetooth
- NFC

حذف:

- Facebook / TikTok (اكبر أدوات التتبع).

تقليل التتبع الشبكي:

استخدم دائمًا: Proton VPN.

ويفضل: عدم استخدام نفس الشبكات دائمًا.

استراتيجية "الهاتفين" (مهم جدًا)

هاتف 1:

- عادي (تطبيقات – حسابات).

هاتف 2:

- نظيف (بدون حسابات شخصية).
- يستخدم فقط للأشياء الحساسة.

هذه أقوى طريقة يستخدمها المحترفون.

طبقة إضافية قوية:

استخدم Faraday عند الحاجة:

- Mission Darkness TitanRF Faraday Sack

هذا يقطع التتبع 100% وقت الإغلاق

الحقيقة المهمة:

- لا يوجد شيء "غير قابل للتتبع 100%"
- لكن يمكنك الوصول إلى: **صعب جدًا – مكلف جدًا – شبه مستحيل عمليًا**

خلاصة مهمة قوية

إذا أردت أقصى حماية، استخدم:

1. نظام مثلGrapheneOS .
2. VPNدائم.
3. هاتف منفصل.
4. حقيبةFaraday>
5. سلوك واعي

المؤكد أن أغلب الاختراقات تأتي من:

- روابط
- تطبيقات
- أخطاء بشرية

☞وليس من "اختراق خارق"

المحور الرابع: كيف يتم التجسس (الطرق الحقيقية):

أولًا: كيف يتم التجسس فعليًا (الحقيقة)

أهم حقيقة: 90% من التجسس عبارة عن خداع المستخدم، وليس اختراق "خارِق"

كيف يتم ذلك؟

1- الروابط الخبيثة (أخطر شيء): تصلك رسالة:

- واتساب – إيميل – SMS.
- تضغط الرابط فيتم تثبيت برنامج تجسس.

هذه الطريقة تُستخدم حتى في هجمات متقدمة

2-التطبيقات المزيفة: تطبيق يبدو عادي:

- لعبة.
- VPN مزيف.
- نسخة معدلة.

لكنه يحتويSpyware

3-شبكات WiFi المزيفة: شبكة باسم:

- "Free Airport WiFi"

يتم اعتراض:

- كلمات المرور
- البيانات

4- الهندسة الاجتماعية(Social Engineering): شخص يقنعك:

- تحميل ملف.
- إعطاء كود.
- تثبيت تطبيق.

هذا أخطر من أي تقنية

5- تتبع عبر الشبكة (بدون اختراق): حتى بدون اختراق:

- الأبراج (Cell towers) تعرف موقعك.
- GPS يعمل باستمرار.
- التطبيقات ترسل بياناتك.

هذا يسمى: **Tracking وليس Hacking**

6- هجمات متقدمة (نادرة جدًا)

مثل:

- Pegasus spyware
  - لا تحتاج ضغط رابط.
  - تستغل ثغرات في النظام.

لكنها:

- تُستخدم ضد أهداف عالية جدًا.
- مكلفة جدًا (ملايين الدولارات).

ثانيًا: كيف تحمي نفسك عمليًا (ضد كل هذا)

قاعدة ذهبية: إذا لم تضغط، لن تُخترق غالبًا.

أهم 5 قواعد: 1- لا تضغط أي رابط مشبوه: حتى لو من صديق. 2- لا تثبت تطبيق خارج المتجر الرسمي: حتى المتجر الرسمي ليس آمن 100%. 3- استخدم: Signal بدل واتساب عند الحاجة – Proton VPN. 4- حدث النظام دائمًا: Android – iOS : التحديث يؤدي إلى إغلاق الثغرات. 5- استخدم حقيبة Faraday عند الشك: مثل Mission Darkness TitanRF Faraday Sack يعزل الجهاز تمامًا.

المستوى الاحترافي opSec: كيف يفكر المحترفون:

- لا يستخدمون جهاز واحد لكل شيء.
- لا يربطون كل حساباتهم ببعض.
- لا يثقون بأي شبكة.

نموذج عملي قوي جدًا: جهازان:

الأول: جهاز نظيف:

- بدون حسابات
- بدون تطبيقات غير ضرورية

الثاني: جهاز عادي:

- للحياة اليومية

الحقيقة التي يجب أن تعرفها: لا أحد يراقبك "بشكل متقدم" إلا إذا كنت:

- هدف مهم جدًا.
- أو قمت بشيء حساس جدًا.

أهم استنتاج: الخطر الحقيقي عليك يأتي من تطبيق مزيف أو رابط فقط.
وليس من: قمار صناعية ولا اختراقات خيالية.

خلاصة ذهبية: أنت أقوى من 95% من المستخدمين أمنا إذا طبّقت:

- لا تضغط روابط.
- استخدمVPN.
- حدّث جهازك.
- استخدم Faraday عند الحاجة.

تذكير سريع (الخلاصة الذهبية):

- لا تضغط روابط مشبوهة.
- لا تثبت تطبيقات غير موثوقة.
- استخدم VPN عند الحاجة.
- استخدم حقيبة Faraday في الحالات الحساسة.
- افصل بين حياتك الرقمية (عمل / شخصي).

بهذه الأشياء البسيطة نسبيًا، أنت فعلًا في مستوى أمان عالٍ جدًا.

فكرة أخيرة مهمة: الأمان ليس "خوف..." بل هو **إدارة ذكية للمخاطر**

يعني:

- تعيش حياتك طبيعي.
- لكن بدون سذاجة رقمية.

المحور الخامس: تنبيه مهم بخصوص العالية الكاملة لحقيبة فرادي ودورها عزل الموبايل

"يجب التنبيه بخصوص حقيبة فارداي بان الحقيبة تقوم بعزل الاشارات وقطع الاتصال فقط ولا تقوم بعزل الصوت *في حالات الاختراق المتقدمة لأجهزة الموبايل لا يكفي العزل فقط .. لان حقيبة فارداي تعزل الإشارة ولا تعزل الصوت. يعني يمكن تسجيل الصوت في محيط الهاتف في حال وجود برمجيه خبيثة بسيطة على الهاتف .. وتحتفظ بالتسجيلات على الجهاز .. وعند عودة الاتصال والإشارة للهاتف تقوم بإرسالها للمخترق وبالتالي وجب التنويه لهذه النقطة .. لان الناس تستخدم الحقيبة وتعتقد انها في أمان كامل .. بينما تكون ثغره خطيره جدا، وقد سجل حالات تجسس خطيرة بمثل هذه الحالة."

واستدراكا على ما جاء في الورقة الموزعة في الموضوع، فإن ما يأتي يكون مستحقا لأهميته العملية في توفير الحماية المنشودة.

هنا سؤال:

كيف يتم تشغيل الميكروفون سرًا؟

وكيف تكتشفه عمليًا (وليس فقط نظريًا)؟

الإجابة:

أولًا: كيف يتم تشغيل الميكروفون سرًا؟

الفكرة الأساسية: أي تطبيق أو برمجية خبيثة تحتاج: إذن الوصول للميكروفون(Microphone Permission),

الطرق الفعلية المستخدمة في هكذا حالة:

1- تطبيق خبيث بصلاحيات: أكثر سيناريو شائع:

- تطبيق عادي (لعبة/ أداة) – يطلب إذن الميكروفون – يعمل في الخلفية ويسجل.

2- استغلال تطبيق موثوق: هذا نادر، ولكنه ممكن:

- استغلال ثغرة في تطبيق مثل: واتساب / متصفح.
- تشغيل الميكروفون بدون علمك.

3- Spyware متقدم: مثل Pegasus spyware

يستطيع: تشغيل الميكروفون – الكاميرا – قراءة كل شيء.

لكن: يستهدف أشخاص محددين جدًا.

ثانيًا: كيف تكتشفه عمليًا:

العلامة الأهم التي يجب الانتباه لها: سواء على Android أم iOS

ظهور مؤشر الميكروفون (نقطة خضراء أو برتقالية)

- إذا ظهر بدون سبب يؤشر إلى وجود خطر.
- يجب تحقق فورًا من التطبيق المستخدم.

عليك إجراء تحقق يدوي سريع كالآتي:

على:Android

- Settings → Privacy → Permission Manager → Microphone

على:iPhone

- Settings → Privacy & Security → Microphone

راقب: من لديه صلاحية؟ وهل يحتاجها فعلًا؟

اختبار ذكي للتأكد:

1. ضع الهاتف على الطاولة.
2. لا تستخدمه

راقب:

- هل يظهر مؤشر الميكروفون؟
- هل يسخن الجهاز؟

إذا نعم: عليك إجراء تحقق فوري.

مراقبة الشبكة:

- استخدم : (Proton VPN – NetGuard(Android

إذا تطبيق يرسل بيانات بدون سبب يكون مشبوها.

اختبار احترافي بسيط:

تجربة عملية:

1. أغلق الإنترنت (وضع الطيران).
2. ضع الهاتف بجانبك.
3. تحدث بصوت واضح.

ثم:

- أعد تشغيل الإنترنت.
- راقب استهلاك البيانات.

إذا زاد فجأة ← احتمال وجود نشاط

ليس دليل قاطع، لكنه مؤشر.

كيف تمنع تشغيل الميكروفون نهائيًا:

1-إلغاء الصلاحيات: أهم خطوة:

- لا تعطي الميكروفون إلا تطبيقات ضرورية جدًا.

2- استخدم النظام بشكل ذكي:

- في: Android
  - ❖ استخدم "Allow only while using app"
- في: iOS
  - ❖ اختر "Never" لمعظم التطبيقات

3- الحل الفيزيائي (الأقوى):

- إطفاء الهاتف.
- أو استخدام :

❖ Purism Librem 5 (Kill switch)

أهم تحذير: إذا جهازك مخترق ببرمجية متقدمة:

- قد لا ترى أي مؤشر.
- وقد لا تكتشفه بسهولة.

هنا الحل الوحيد: إعادة ضبط المصنع أو تغيير الجهاز.

الخلاصة الاحترافية:

تشغيل الميكروفون سرًا: ممكن.

واكتشاف ذلك: ممكن في أغلب الحالات.

ومنعه أيضا: سهل إذا كنت واعي.

أهم قاعدة في العالم الأمني: "إذا لم تعطه إذن... لا يستطيع استخدامه".

كيف تنشئ بيئة اجتماع "شبه آمنة 100%" ضد التسجيل والتتبع والتسريب.

هذا مستوى احترافي حقيقي تستخدمه الشركات والجهات الحساسة.

الفكرة الأساسية: لا تعتمد على أداة واحدة، بل عليك بناء طبقات حماية(Layers)

الطبقة 1: التحكم في الأجهزة (أهم خطوة)

القاعدة الذهبية: لا يُسمح بأي هاتف داخل الاجتماع

الخيارات:

الأفضل: ترك الهواتف خارج الغرفة

بديل:

- وضعها داخل : Mission Darkness BlockBox Touch

هذا يمنع: الاتصال - وإرسال البيانات.

لكن تذكر: لا يمنع التسجيل الداخلي (كما تعلمنا).

الطبقة 2: منع التسجيل الصوتي:

الحل الاحترافي: قبل الاجتماع عليك التأكد من:

- إطفاء جميع الأجهزة

- أو التأكد من عدم وجودها أساسًا

حلول إضافية تستخدم أحيانًا:

- تشغيل "ضجيج أبيض (White Noise)" خفيف لتشويش أي تسجيل محتمل.

الطبقة 3: تأمين الغرفة:

تحقق من:

- عدم وجود: أجهزة تسجيل مخفية – كاميرات صغيرة.
- إغلاق: أي أجهزة ذكية (– Alexa – TVإلخ).

الطبقة 4: عزل الاتصالات:

إجراءات:

- إيقاف : Bluetooth – WIFI
- أو استخدام غرفة بدون تغطية شبكة

بعض الجهات تستخدم "غرف معزولة إشعاعيًا"

الطبقة 5: العامل البشري (الأخطر):

أهم نقطة: التسريب غالبًا يأتي من الأشخاص وليس الأجهزة

لذلك لا بد من:

- تحديد من يحضر الاجتماع
- منع دخول أشخاص غير موثوقين
- عدم مشاركة المعلومات خارج الاجتماع

نموذج احترافي جاهز

سيناريو مثالي:

1. منع إدخال الهواتف
2. أو وضعها في صندوق Faraday
3. إطفاء جميع الأجهزة
4. تعطيل الشبكات
5. حضور محدود

يعد هذا مستوى أمان عالي جدًا.

أخطاء شائعة:

- الاعتماد على Faraday فقط.
- ترك الهاتف "صامت" فقط.
- الثقة بأن "لا أحد يسجل".

هذه أكبر الثغرات.

الخلاصة القوية:

الأمان الحقيقي للاجتماعات تتمثل في:

- منع الأجهزة.
- تقليل الأشخاص.
- التحكم في البيئة.

الحقيقة النهائية:

حتى أقوى الحكومات لا تعتمد على جهاز واحد، بل على "إجراءات + سلوك + بيئة".

قائمة فحص احترافية (Checklist) للاستخدام قبل أي اجتماع حساس لضمان أعلى مستوى أمان ممكن:

قائمة فحص أمان الاجتماعات الحساسة:

1-قبل الاجتماع (التحضير):

أ. الأجهزة

- منع إدخال الهواتف إلى الغرفة
- أو وضعها داخل صندوق فاراداي
- التأكد من إطفاء: الهواتف، الساعات الذكية، السماعات.

ب. الاتصالات

- إيقاف WiFi – إيقاف Bluetooth – التأكد من عدم وجود تغطية شبكة قوية داخل الغرفة.

ت. المكان

- تفتيش الغرفة بصريًا
- التأكد من عدم وجود: كاميرات مخفية – أجهزة تسجيل.
- إغلاق أو فصل: التلفاز – الأجهزة الذكية (Alexa / Google Home)

2- أثناء الاجتماع:

أ. التعامل مع الحضور:

- التأكد من هوية جميع الحاضرين.

- منع دخول أي شخص غير مصرح له.
- تقليل عدد الحضور قدر الإمكان.

ب. الصوت:

- عدم وجود أي جهاز تسجيل ظاهر.
- (اختياري) تشغيل ضجيج أبيض خفيف.

ت. المعلومات:

- عدم استخدام أوراق حساسة إلا للضرورة.
- منع التصوير أو النسخ.

3-بعد الاجتماع:

أ. المعلومات:

- جمع جميع الأوراق.
- إتلاف أي ملاحظات حساسة (إن لزم).

ب. الأجهزة:

- إعادة الأجهزة لأصحابها.
- عدم مناقشة تفاصيل الاجتماع عبر الهاتف.

4- قواعد ذهبية (مهمة جدًا):

- لا تثق بأي جهاز إلكتروني 100 %.
- لا تعتمد على حقيبة Faraday وحدها.
- الخطر الأكبر من العنصر البشري.
- كلما قلّ عدد الأشخاص زاد الأمان.

استخدام الموبايل القديم وأثر ذلك في الحماية من التتبع

استخدام هواتف قديمة لا تدعم الإنترنت يمكن أن يقلل بعض أشكال التعقب الرقمي، لكنه لا يمنع التعقب بالكامل. إذا كان المقصود بالهواتف "الهواتف التقليدية (Feature Phones) "التي تقتصر على المكالمات والرسائل النصية، فهناك عدة نقاط مهمة:

- يختفي جزء كبير من التعقب المرتبط بالتطبيقات والإنترنت:

❖ لا توجد تطبيقات تجمع بيانات الموقع أو جهات الاتصال أو سجل التصفح.

❖ لا توجد خدمات سحابية أو حسابات مرتبطة بالهاتف كما في الهواتف الذكية.

❖ لكن شبكة الهاتف نفسها ما زالت قادرة على تحديد الموقع التقريبي للجهاز:

- أي هاتف يعمل بشريحة اتصال يتواصل باستمرار مع أبراج الاتصالات القريبة.
- يمكن لمشغل الشبكة معرفة المنطقة التي يوجد فيها الهاتف، وأحيانًا بدقة أعلى حسب كثافة الأبراج.
- سجلات المكالمات والرسائل تبقى موجودة لدى شركات الاتصالات وفق القوانين المحلية.

- لا يمنع ذلك وسائل تعقب أخرى:

- إذا كان الهاتف مزودًا بنظام GPS (بعض النماذج القديمة تحتوي عليه) فقد تكون هناك إمكانيات إضافية لتحديد الموقع.
- يمكن ربط أنماط الاستخدام وهوية الشريحة بصاحب الهاتف.

لذلك، من الناحية التقنية، الانتقال من الهواتف الذكية إلى هواتف بسيطة يقلل "البصمة الرقمية" بشكل واضح، لكنه لا يجعل المستخدم غير قابل للتعقب أو المراقبة تمامًا.

القول الأدق هو: "يقلل من بعض أنواع التعقب، ولا يلغيها".

أما فيما يتعلق بحركة طالبان تحديدًا، فقد أشارت تقارير إعلامية خلال السنوات الأخيرة إلى تشجيع بعض المسؤولين على استخدام هواتف أبسط لأسباب تتعلق بالأمن وتقليل مخاطر الاختراق أو جمع البيانات عبر التطبيقات، لكن السبب المعلن في هذه التقارير كان تقليل التعرض للمراقبة الرقمية الحديثة، وليس لأن الهواتف القديمة توفر حصانة كاملة من التعقب.

باختصار:

هل يمنع الإنترنت؟ نعم، إذا كان الهاتف لا يدعم الإنترنت.

هل يمنع تعقب التطبيقات؟ إلى حد كبير.

هل يمنع تحديد الموقع عبر شبكة الاتصالات؟ لا.

هل يجعل الشخص غير قابل للتعقب؟ لا، لكنه قد يقلل بعض المخاطر التقنية مقارنة بالهواتف الذكية.

المحور السادس: توضيح المصطلحات الواردة في المادة

1- العمليات، الاستخبارات، والأمن التشغيلي

- **الأمن التشغيلي (OpSec):** مجموعة من الإجراءات والتدابير التي يتخذها الأفراد لحماية معلوماتهم وسلوكياتهم اليومية، ومنع الخصوم من ربط خيوط غير مباشرة قد تكشف عن هوياتهم أو تحركاتهم.
- **الاستخبارات مفتوحة المصدر :(OSINT)** عملية جمع وتحليل المعلومات المتاحة علناً للعموم (مثل وسائل الإعلام، وسائل التواصل، السجلات الحكومية المفتوحة) لاستخراج تقارير استخباراتية دون الحاجة لاختراق.
- **شبكة "العيون الخمس (Five Eyes):** "تحالف استخباراتي يضم خمس دول (الولايات المتحدة، بريطانيا، كندا، أستراليا، نيوزيلندا) لتبادل المعلومات الاستخباراتية والإشارات الإلكترونية على مستوى عالمي.
- **مركز" (GCHQ):** مقر الاتصالات الحكومية" البريطاني، وهو وكالة الاستخبارات والأمن المسؤولة عن تقديم التجسس الإلكتروني (استخبارات الإشارات) وحماية أمن المعلومات للحكومة والجيش البريطاني.

2-الهواتف، العتاد، وأمن الأجهزة الإلكترونية

- **الهواتف الحارقة / النظيفة (Burner Phones):** هواتف رخيصة ومسبقة الدفع تُشترى نقداً وتُستخدم لفترة وجيزة أو لمهمة محددة ثم يتم التخلص منها (حرقها) لضمان عدم ربطها بهوية المستخدم الحقيقية.
- **الهواتف ذات المفاتيح الفيزيائية (Hardware Kill Switches):** مفاتيح حقيقية (أزرار ميكانيكية) موجودة على جسم الهاتف، تسمح بقطع الطاقة تماماً وفصل الكاميرا، الميكروفون، أو الشريحة ميكانيكياً، مما يمنع أي برمجية اختراق من تشغيلها سراً.
- **كسر الحماية (Root / Jailbreak):** عملية تعديل نظام تشغيل الهاتف Root) للأندرويد، (Jailbreak للآيفون لإلغاء القيود التي تفرضها الشركة المصنعة، مما يمنح المستخدم صلاحيات كاملة، لكنه في الوقت ذاته يضعف دفاعات الهاتف الأمنية.
- **تقنية Knox العسكرية:** نظام أمني متكامل ومدمج في عتاد (Hardware) وبرمجيات أجهزة سامسونج، يوفر بيئة معزولة تماماً لحماية البيانات الحساسة من الاختراق حتى لو تعرض نظام التشغيل الأساسي للتهديد.
- **وضعية "التسطيح (Lay it Flat):** "أسلوب أمني يتضمن وضع الهاتف بشكل مسطح تماماً على السطح لتقليل زاوية رؤية الكاميرات، أو لتغطية الميكروفونات، أو لمنع مستشعرات الحركة من التقاط أي اهتزازات قد تُترجم إلى مدخلات.

3-التهديدات، الاختراقات، والبرمجيات الخبيثة:

- **يوم الصفر (Zero-day):** ثغرة أمنية مكتشفة حديثاً في نظام أو برنامج لا تعلم عنها الشركة المصنعة شيئاً، وبالتالي يوجد "صِفر" يوم من الوقت لإصلاحها، وتُستغل من قِبل المهاجمين قبل سدّها.
- **هجمات النقر الصفري (Zero-click):** من أخطر أنواع الاختراقات، حيث يتم اختراق جهاز الضحية (عبر إرسال رسالة أو ملف خفي) دون أن يتطلب ذلك من المستخدم الضغط على أي رابط أو التفاعل مع الرسالة.

- **الروتكيت (Rootkit):** برمجية خبيثة متطورة للغاية تتسلل إلى أعمق مستويات نظام التشغيل (الجذور)، وتتميز بقدرتها الفائقة على إخفاء نفسها وأنشطتها تماماً عن برامج مكافحة الفيروسات التقليدية.
- **برمجيات سرقة البيانات البسيطة (Infostealers):** نوع من البرمجيات الخبيثة المصممة لغرض محدد وسريع: تفتيش الجهاز وسرقة كلمات المرور المحفوظة، وبيانات المتصفح، وملفات تعريف الارتباط (Cookies)، ثم إرسالها للمهاجم.
- **تبديل الشريحة (SIM Swapping):** هجوم يعتمد على الهندسة الاجتماعية، حيث يقنع المهاجم شركة الاتصالات بنقل رقم هاتف الضحية إلى شريحة جديدة يملكها المهاجم، بهدف سرقة حساباته التي تعتمد على الرسائل النصية لتأكيد الهوية.
- **Juice Jacking:** نوع من الاختراق يحدث عند توصيل الهاتف بـ "شواحن عامة" (مثل الموجودة في المطارات)، حيث يتم استغلال سلك الشحن لنقل برمجيات خبيثة إلى الهاتف أو سرقة البيانات منه أثناء شحنه.
- **أبواب خلفية مخفية (Backdoors):** ممرات أو منافذ سرية يتم زرعها عمداً في البرامج أو العتاد من قبل المطورين أو الوكالات الاستخباراتية، تتيح لهم الدخول إلى النظام وتخطّي العقبات الأمنية في أي وقت دون علم المستخدم.
- **مؤشرات الاختراق (IOCs):** الأدلة الرقمية والآثار التي تتركها البرمجيات الخبيثة وراءها داخل النظام)مثل عناوين IP مشبوهة، أو ملفات غريبة(، وتُستخدم من قبل خبراء الأمن لإثبات وقوع الاختراق.
- **مجموعات قراصنة صينيين Volt Typhoon و Salt Typhoon:** مجموعات تسلل إلكتروني متطورة (مدعومة من دول)؛ تركز **Volt Typhoon** على اختراق البنية التحتية الحيوية (كالطاقة والمياه)، بينما تركز **Salt Typhoon** على اختراق شبكات الاتصالات ومزودي خدمات الإنترنت للتجسس.

4-أدوات التشفير وإدارة الهوية الرقمية:

- **الثقة الصفرية (Zero Trust):** نموذج أمني يرفع شعار "لا تثق بأحد أبداً، وتحقّق دائماً". بموجبه، لا يتم الوثوق بأي مستخدم أو جهاز تلقائياً حتى لو كان داخل شبكة العمل، بل يجب التحقق من هويته وصلاحياته عند كل خطوة.
- **التشفير من الطرفين (End-to-End Encryption):** تقنية تضمن أن الرسائل يتم تشفيرها على جهاز المرسل ولا يتم فك تشفيرها إلا على جهاز المستقبل، بحيث لا يستطيع أي طرف وسيط (حتى الشركة المطورة للتطبيق) قراءتها.
- **تطبيقات الـ VoIP المشفرة ومكالمات البيانات:** تطبيقات تتيح إجراء المكالمات الصوتية والمرئية عبر الإنترنت (VoIP) مع تشفير هذه البيانات الصوتية لمنع التنصت عليها أثناء انتقالها عبر الشبكة.
- **AES-256:** معيار التشفير المتقدم بطول مفتاح 256 بت. يُعد أحد أقوى بروتوكولات التشفير المتناظر في العالم، وتستخدمه الحكومات والجيوش لحماية البيانات الحساسة، ويستحيل كسر دفاعاته بالحواسب الحالية.
- **أداة BitLocker:** ميزة أمنية مدمجة في نظام تشغيل "ويندوز" تقوم بتشفير القرص الصلب كاملاً لحماية البيانات من السرقة أو الاطلاع عليها في حال فُقد الجهاز أو سُرق.

- **مولد كلمات المرور (Generator):** أداة ذكية تقوم بإنشاء كلمات مرور عشوائية معقدة وطويلة للغاية (تتكون من رموز، أرقام، وحروف كبيرة وصغيرة) يصعب تخمينها أو كسرها.
- **منصات إدارة كلمات المرور:**
  - **Bitwarden:** مدير كلمات مرور مفتوح المصدر وموثوق، يقوم بتشفير وحفظ كلمات المرور سحابياً مع إمكانية المزامنة بين مختلف الأجهزة.
  - **Password1:** مدير كلمات مرور تجاري يتميز بواجهة قوية ومزايا أمنية متقدمة لحماية الهويات الرقمية للشركات والأفراد.
  - **KeePassXC / KeePassDX:** نسخ حديثة من مدير كلمات المرور الكلاسيكي (KeePass.)يمتاز بأنه **محلي تماماً** (لا يرفع بياناتك على السحاب)، حيث تحتفظ بملف كلمات المرور المشفر تحت سيطرتك الكاملة XC) للكمبيوتر و DX للأندرويد.(
- **وضع السفر (Travel Mode):** ميزة في برامج إدارة كلمات المرور مثل **Password1** تقوم بحذف البيانات الحساسة مؤقتاً من الجهاز أثناء عبور الحدود والمطارات، ويمكن استعادتها بضغطة زر بعد تجاوز التفتيش.
- **Vanish Mode وضع الاختفاء:** ميزة في تطبيقات المراسلة (مثل إنستجرام وماسنجر) تجعل الرسائل المقروءة تختفي وتُحذف تماماً بمجرد إغلاق نافذة المحادثة، ولا تترك أي أثر في سجلات التطبيق.

5-الصوتيات والخصوصية الفيزيائية

- **الضوضاء البيضاء (White Noise) وأجهزتها:** ترددات صوتية عشوائية ومستمرة تدمج جميع الترددات التي تسمعها الأذن البشرية معاً (مثل صوت المطر أو جهاز التكييف). تُستخدم أجهزتها في الغرف الأمنية لتشويش ميكروفونات التجسس وأجهزة التنصت الليزرية ومنعها من التقاط الأصوات أو وضوح الكلام البشري.

6-الذكاء الاصطناعي والتزييف:

- **التزييف العميق (Deepfakes):** تقنية تعتمد على الذكاء الاصطناعي لإنشاء مقاطع فيديو أو صور أو تسجيلات صوتية مزيفة ومقنعة للغاية، تظهر أشخاصاً حقيقيين يقولون أو يفعلون أشياءً لم يقولوها أو يفعلوها في الواقع.
- **مكتشفات التزييف العميق (Deepfake Detectors):** برمجيات وأدوات متطورة تعتمد بدورها على الذكاء الاصطناعي لتحليل الوسائط وكشف التعديلات الدقيقة غير المرئية بالعين المجردة، لتحديد ما إذا كان الفيديو أو الصوت حقيقياً أم مزيفاً.

7-فضاء الإنترنت المظلم:

- **الإنترنت المظلم (Dark Web):** جزء مخفي من شبكة الإنترنت لا يمكن الوصول إليه عبر المتصفحات العادية (مثل جوجل كروم)، ويتطلب متصفحات خاصة) مثل .(Tor يوفر ميزة التخفي التام للمستخدمين والمواقع، ولذلك يُستغل في الأنشطة المشروعة التي تتطلب سرية مطلقة، وكذلك في الأنشطة غير القانونية.

8-التشفير والحوسبة الكمية (المستقبلية):

- **الحواسيب الكمية (Quantum Computers):** جيل جديد من الحواسيب فائقة القوة تعتمد على قوانين ميكانيكا الكم. تمتلك قدرات معالجة هائلة تتيح لها كسر معظم خوارزميات التشفير التقليدية المستخدمة حالياً في ثوانٍ معدودة.
- **التشفير الكمي (Quantum Encryption):** علم استخدام الخصائص الفيزيائية الكمية لحماية البيانات وتأمين القنوات الاتصالية بطريقة تجعل من المستحيل فيزيائياً اعتراضها دون كشف المتسلل.
- **توزيع المفتاح الكمي (QKD):** طريقة آمنة لتبادل مفاتيح التشفير بين طرفين باستخدام فوتونات الضوء. إذا حاول أي طرف ثالث التجسس أو اعتراض المفتاح أثناء إرساله، تتغير الحالة الفيزيائية للفوتونات فوراً، مما ينبه الطرفين ويلغي المفتاح تلقائياً.
- **بروتوكول PQ3:** بروتوكول تشفير متطور جداً أطلقته شركة أبل لحماية تطبيق(iMessage) ، يعتمد على نظام "التشفير ما بعد الكم" لمقاومة أي هجمات فك تشفير قد تشنها الحواسب الكمية المستقبلية.
- **التشفير ما بعد الكم (Post-Quantum Cryptography):** تطوير خوارزميات ومعادلات رياضية جديدة ومعقدة لتشغيلها على الحواسيب الحالية، بهدف تأمين البيانات وجعلها مستعصية على الكسر حتى أمام الحواسيب الكمية فائقة القدرة.
- **القمر الاصطناعي "ميسيوس (Micius):** "قمر اصطناعي صيني أُطلق كأول مختبر فضائي في العالم مخصص لتجارب التشفير الكمي، ونجح في إرسال مفاتيح تشفير كمية غير قابلة للاختراق عبر مسافات شاسعة بين الفضاء والأرض.

المحور السابع: صور تطبيقية

صندوق فارادي – حقائب فارادي





شنطة فاراداي كبيرة جدا للابتوب (20 انش × 15 انش)، قفص فاراداي مع مقبض، شنطة حماية فاراداي لحجب الاشارة، شنطة حماية ضد السرقة والاختراق، مقاومة للحريق والماء (فضي)



حقبة فارادي لريموت السيارة

